



vGW Series Settings and Reports



Published: 2013-07-25

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2013, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

vGW Series Settings and Reports
Copyright © 2013, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xi
	Documentation and Release Notes	xi
	Documentation Conventions	xi
	Documentation Feedback	xiii
	Requesting Technical Support	xiii
	Self-Help Online Tools and Resources	xiv
	Opening a Case with JTAC	xiv
Part 1	Basics	
Chapter 1	Settings Module Basics	3
	Understanding the vGW Series Settings Module	3
Part 2	Application Settings	
Chapter 2	Basics	7
	Understanding the vGW Series Application Settings	7
Chapter 3	Status and Licenses	9
	Viewing Status and License Information Using the vGW Series Settings Module	9
	Understanding Licenses for the vGW Series	10
	License Requirements	10
	vGW Series Licenses	10
	Evaluation Licenses	11
	Obtaining, Installing, and Managing vGW Series Licenses	11
Chapter 4	Installation	13
	Configuring vGW Series Installation Settings	13
	Installing vGW Security VMs on ESX/ESXi Hosts	15
	Understanding vGW Series Timeout Parameters and the vGW Security VM Installation, Uninstallation, and Update Tasks	21
	Securing and Unsecuring Virtual Machines Using the vGW Security Design VM	22
	Understanding Automatic Securing of VMs	23
	Understanding the VMware Auto Deploy Feature for ESXi Servers and vGW Series Integration With It	25
	VMware Auto Deploy Feature	25
	vGW Series Support for Auto Deploy	25

	vGW Series Automatic Installation of vGW Security VMs	25
	Configuring VMware Auto Deploy and vGW Series to Automatically Secure ESXi	
	Hosts Provisioned by Auto Deploy	26
	Configuring Auto Deploy in VMware	27
	Configuring vGW Series to Support Auto Deploy	31
	Disabling the vGW Series Suspend-Resume Process Enacted After a VM Is	
	Unsecured	34
	Displaying the State of the vmsafe config Setting	34
	Disabling the Suspend-Resume Process	35
	Removing vGW Security VMs from ESX/ESXi Hosts	36
	Integrating the vGW Series with VMware Using the Settings Module	37
	Understanding vGW Series Integration with vCloud Director	41
	VMware vCloud Director	41
	vGW Series and vCloud	41
	Requirements	42
	Configuring vGW Series Integration with vCloud Director	43
Chapter 5	Policy-per-vNIC Feature	47
	Understanding the vGW Series Policy per vNIC Feature	47
	About Policy per vNIC	47
	Why Use Policy per vNIC	48
	vNICs With Individual Policies and Smart Groups	49
	Viewing vNICs With Individual Policies	49
	Naming Conventions for vNICs	50
	Configuring the vGW Series Policy per vNIC Feature	50
	Configuring and Displaying vGW Policies for Individual vNICs on the Same	
	VM	52
	Configuring Policy per vNIC to Secure Only Some of a VM's vNICs	55
	Understanding Policy per vNIC and Smart Groups for VMware Environments . . .	55
Chapter 6	Split-Center and Multi-Center Features	59
	Understanding the vGW Series Split-Center Feature	59
	Understanding the Multi-Center Feature	63
	The Multi-Center Feature	64
	Deploying vGW Series in an Environment With a Mix of Delegate and	
	Stand-alone vGW Security Design VMs in Various vCenters	65
	Configuring vGW Series Multi-Center	66
	vGW Security Design VM Master Center	66
	vGW Security Design VM Delegate Centers	66
	Configuring Multi-Center	67
	Understanding vGW Series Multi-Center Synchronized Objects	69
	Object Synchronization	69
	Object Naming	70
	Creation of Objects Local to the Delegate vGW Security VM	70
	Configuring Scaling Using the Multi-Center and Split-Center Features	70
Chapter 7	Administrators Definitions and Permissions	79
	Adding New vGW Series Administrator Definitions, Permissions, and Authorization	
	Using the Settings Module	79
	Setting Up Active Directory for vGW Series Administrator Authentication	83

Chapter 8	Machine Definitions for VMs and Other Resources	85
	Adding and Editing vGW Series Machines Definitions (VMware)	85
	Adding a Machine	85
	Viewing Machine Information	87
Chapter 9	E-Mail and Reporting	89
	Configuring vGW Series E-Mail and Reporting Applications Settings	89
Part 3	Security Settings	
Chapter 10	Getting Started	93
	Understanding the vGW Series Security Settings	93
	Configuring Global Settings Using the vGW Series Settings Module	94
	Understanding the vGW Security VM Settings	97
Chapter 11	Antivirus and IDS Settings	103
	Understanding and Configuring the vGW Series AntiVirus Settings	103
	Understanding and Configuring IDS Settings	104
	Understanding and Configuring IDS Signatures Settings	107
Chapter 12	Groups	111
	Understanding vGW Series Groups	111
	Uses of Groups	111
	vGW Series Group Types	112
	Policy Groups and Monitoring Groups	112
	Defining the Group as a Policy Group Option with Automatic or Manual Selected	112
	Copying Groups	113
	Creating vGW Series Smart Groups for VMware	114
	vGW Series Attributes for VMware	118
	About Using vGW Series Attributes for VMware	123
	Automatically Applying Policy Rules to VMs in Policy Groups	124
Chapter 13	Alerts	127
	Understanding the vGW Series Security Alert Settings	127
	Event Types	127
	E-mail Alert Settings	127
	SNMP Trap Settings	128
	AutoConfig and Multicast Alerts	128
Chapter 14	SRX Series Devices	129
	Understanding the vGW Series SRX Zones Settings	129
Chapter 15	Networks and Protocols	131
	Understanding the Settings Module Networks Settings	131
	Understanding vGW Series Protocols Support	131
Part 4	Appliance Settings	
Chapter 16	Updates	135
	Understanding the vGW Series Update Settings	135
	Updating the vGW Security Design VM	135

	Updating vGW Security VMs in Batch Mode	137
Chapter 17	Networks and Proxies	139
	Configuring the vGW Series Network Settings	139
	Configuring vGW Series Proxy Settings	142
Chapter 18	Time	143
	Configuring vGW Series Time Settings	143
Chapter 19	Backup and Restore	145
	Understanding the vGW Series Backup and Restore Feature	145
	Configuring the vGW Series Backup and Restore Feature	147
Chapter 20	Logs	151
	Understanding vGW Series Log Collection	151
	Log Collection	151
	Generating the Log Collections	152
	Uploading the File	153
	Downloading the File	153
	Using a Method Other Than the vGW Security Design VM to Generate Log Collections for It	153
	Viewing the vGW Series Logs	154
Chapter 21	Support	155
	Understanding vGW Series Support Settings	155
Part 5	Reports	
Chapter 22	Basics	159
	Understanding the vGW Series Reports Module	159
	Configuring a vGW Series Report	160
	Configuring Specifications for Automated Reports Using the vGW Series Reports Module	163
Chapter 23	Reports Configuration	165
	Understanding vGW Series Custom Report Types	165
	Understanding vGW Series Network Reports	166
	About the vGW Series Firewall Reports	166
	About the vGW Series IDS Reports	166
	About the vGW Series Introspection Reports	167
	Understanding the vGW Series Compliance Report	167
	Understanding the vGW AntiVirus Report	168
Part 6	Index	
	Index	171

List of Figures

Part 1	Basics	
Chapter 1	Settings Module Basics	3
	Figure 1: vGW Series Settings Module	3
Part 2	Application Settings	
Chapter 4	Installation	13
	Figure 2: Securing an ESX/ESXi Host With a vGW Security VM	16
	Figure 3: Installing a vGW Security VM on an ESX/ESXi Host	17
	Figure 4: Specifying vGW Security Parameters During Installation	17
	Figure 5: vGW Security VM Installation Process Completion Notice	20
	Figure 6: vGW Series CLI Console	22
	Figure 7: vGW Series Failure Alert for vGW Security VM Installation on Automatically Deployed ESXi Hosts	26
	Figure 8: Configuring Automatic Installation of vGW Security VMs for Auto-Deployed ESXi Hosts	32
	Figure 9: vGW Security VM Uninstall	36
	Figure 10: vGW Security Design VM vCenter Integration Window Showing vCloud Director Settings Pane	44
Chapter 5	Policy-per-vNIC Feature	47
	Figure 11: Policy for Single vNIC	48
	Figure 12: VM with Multiple vNICs Shown in the VM Tree	49
	Figure 13: Policy Per vNIC	51
	Figure 14: Applying Policy to Individual vNICs	52
Chapter 6	Split-Center and Multi-Center Features	59
	Figure 15: Configuring the Management Scope During Installation to Include Clusters	61
	Figure 16: vGW Series Multi-Center	65
	Figure 17: Multi-Center Configuration Page at Master vGW Security Design VM	67
	Figure 18: Delegate Center Configuration on the Master vGW Security Design VM	68
	Figure 19: Delegate Center Configuration on the Master vGW Security Design VM	73
Chapter 7	Administrators Definitions and Permissions	79
	Figure 20: Creating a VM Admin Administrator Account	81
	Figure 21: Adding a New Administrator	82
	Figure 22: Changing the Password for a Defined Administrator	83

Chapter 8	Machine Definitions for VMs and Other Resources	85
	Figure 23: Configuring Machines Information	87
	Figure 24: Syslog Entry Including VM Name and Log Tag	87
Part 3	Security Settings	
Chapter 10	Getting Started	93
	Figure 25: Configuring vGW Series Global Settings	95
	Figure 26: Changing the vGW Security VM Management Interface IP Address . .	98
	Figure 27: Configuring the Security VM Settings Page Console Monitoring	100
	Figure 28: Configuring Network Monitoring for Individual vGW Security VMs . .	101
Chapter 11	Antivirus and IDS Settings	103
	Figure 29: IDS Settings Page	105
	Figure 30: IDS Updates Pane	106
	Figure 31: Signatures in a Signature Group	108
	Figure 32: Signature Details	109
Chapter 12	Groups	111
	Figure 33: Creating a Smart Group Using Basic Mode	115
	Figure 34: The Smart Group Editor in Advanced Mode Using Regular Expressions	117
	Figure 35: Configuring a Smart Group As a Policy Group	125
	Figure 36: Configuring Policy Rules for a Smart Group with Policy Group Enabled	126
Part 4	Appliance Settings	
Chapter 17	Networks and Proxies	139
	Figure 37: Settings Module Network Settings Configuration for Dual Stack Support	141
Chapter 19	Backup and Restore	145
	Figure 38: Settings Module Backup and Restore Settings	146
	Figure 39: Settings Module Backup and Restore Settings	147
Part 5	Reports	
Chapter 22	Basics	159
	Figure 40: Adding a vGW Series Report Using the Reports Module	161
	Figure 41: Defining General, Destination, and Scheduling Information for the Report	161
	Figure 42: Configuring the Report Destination and Generation Schedule	162
	Figure 43: Configuring the Types of Reports to Generate	163

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xii
	Table 2: Text and Syntax Conventions	xii
Part 2	Application Settings	
Chapter 5	Policy-per-vNIC Feature	47
	Table 3: Smart Group Attributes for vNICs When Policy per vNIC Is Enabled	56
Chapter 7	Administrators Definitions and Permissions	79
	Table 4: vGW Series Built-In Administrator User Types	79
Part 3	Security Settings	
Chapter 12	Groups	111
	Table 5: Operators for Creating Smart Groups Using Regular Expression	117
	Table 6: Smart Group Attributes	118

About the Documentation

- Documentation and Release Notes on page xi
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiii

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Documentation Conventions

Table 1 on page xii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: <code>user@host> configure</code>
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies book names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	<code>stub <default-metric metric>;</code>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast <i>(string1 string2 string3)</i>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Basics

- [Settings Module Basics on page 3](#)

CHAPTER 1

Settings Module Basics

- Understanding the vGW Series Settings Module on page 3

Understanding the vGW Series Settings Module

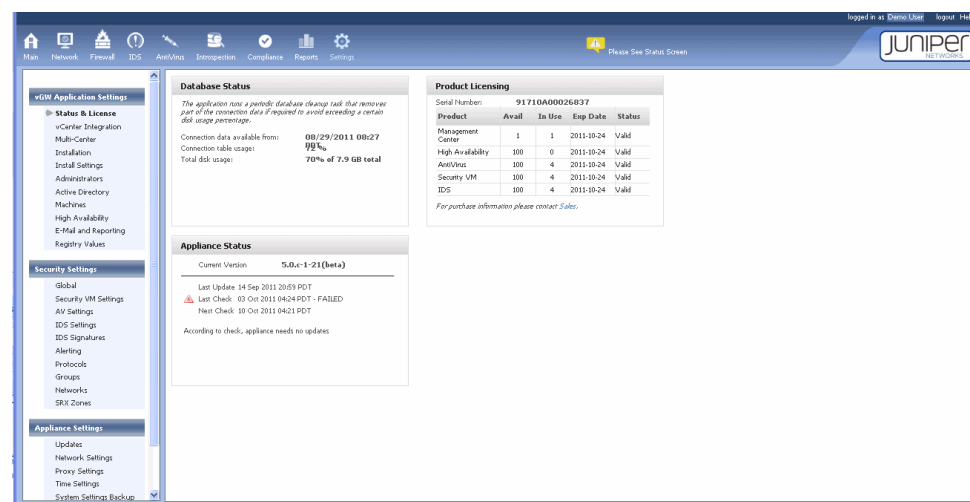
The Settings module of the vGW Security Design VM controls core vGW Series operations. The Settings module covers a wide range of information within its subsections. It contains three subsections each of which allows you to configure or view information about various parts of the system.

The Settings module contains three main sections:

- Application Settings
- Security Settings
- Appliance Settings

Figure 1 on page 3 shows the Settings module. The left navigation pane shows the sections and features that comprise the Settings module.

Figure 1: vGW Series Settings Module



- Related Documentation**
- [Understanding the vGW Series Application Settings on page 7](#)
 - [Understanding the vGW Series Security Settings on page 93](#)

PART 2

Application Settings

- [Basics on page 7](#)
- [Status and Licenses on page 9](#)
- [Installation on page 13](#)
- [Policy-per-vNIC Feature on page 47](#)
- [Split-Center and Multi-Center Features on page 59](#)
- [Administrators Definitions and Permissions on page 79](#)
- [Machine Definitions for VMs and Other Resources on page 85](#)
- [E-Mail and Reporting on page 89](#)

CHAPTER 2

Basics

- [Understanding the vGW Series Application Settings on page 7](#)

Understanding the vGW Series Application Settings

The Settings module Applications section allows you to license the vGW Series product, check status on the vGW Security Design VM, control access to VMware, and add administrator information and modify it. You can also configure machines, high availability support for the vGW Security Design VM, and reporting settings.

The following topics cover specific Applications settings:

- [Viewing Status and License Information Using the vGW Series Settings Module on page 9](#)
- [Understanding Licenses for the vGW Series on page 10](#)
- [Obtaining, Installing, and Managing vGW Series Licenses on page 11](#)
- [Integrating the vGW Series with VMware Using the Settings Module on page 37](#)
- [Understanding the vGW Series Split-Center Feature on page 59](#)
- [“Understanding the Multi-Center Feature” on page 63 and “Configuring vGW Series Multi-Center” on page 66.](#)
- [Configuring Scaling Using the Multi-Center and Split-Center Features on page 70](#)
- [Installing vGW Security VMs on ESX/ESXi Hosts on page 15](#)
- [Configuring vGW Series Installation Settings on page 13](#)
- [Configuring the vGW Series Policy per vNIC Feature on page 50](#)
- [Adding New vGW Series Administrator Definitions, Permissions, and Authentication Using the Settings Module](#)
- [Setting Up Active Directory for vGW Series Administrator Authentication on page 83](#)
- [Understanding the Multi-Center Feature on page 63](#)
- [Configuring vGW Series Multi-Center on page 66](#)
- [Configuring Scaling Using the Multi-Center and Split-Center Features on page 70](#)
- [Configuring vGW Series E-Mail and Reporting Applications Settings on page 89](#)

For details on configuring high availability for the vGW Security Design VM, see *Installing an Additional vGW Security Design VM and Configuring the Primary vGW Security Design VM to Use It for High Availability*.

**Related
Documentation**

- [Understanding the vGW Series Settings Module on page 3](#)
- *Understanding vGW Series*
- *Understanding the vGW Security VM*
- *Understanding the vGW Security Design VM*

CHAPTER 3

Status and Licenses

- [Viewing Status and License Information Using the vGW Series Settings Module on page 9](#)
- [Understanding Licenses for the vGW Series on page 10](#)
- [Obtaining, Installing, and Managing vGW Series Licenses on page 11](#)

Viewing Status and License Information Using the vGW Series Settings Module

The Settings module Applications section allows you to view basic system status, and configure and view licensing information. It contains the following parts:

- **Database Status**—Displays the status of the internal database that stores network session data. When the database disk is full, session data for the oldest sessions is deleted. This section displays how far back session data stored in the database extends.

By default, the disk that contains the vGW Series database is set to 8 GB. If the database is not holding enough information for your environment, you can increase its size.

To increase the database size:

1. Power down the vGW Security Design VM.
2. In VMware, edit settings for the vGW Security Design VM, increasing the size of the second disk.
3. Start the vGW Security Design VM.

When the vGW Security Design VM boots up, the new disk size is recognized, and the database expands into the newly defined space.

- **Appliance Status**—This pane shows the current version of the appliance and the update version. You can use this pane to check if there are updates available that have not yet been applied.
- **Product Licensing**—This area displays a table summarizing valid licenses for the Juniper Networks vGW Series. The licensing system is 'multi-key' meaning you can attach various licenses for features and feature counts to the system.

At minimum, you must have a valid license for the vGW Security Design VM management center.

For information about licenses and specifying them, see:

- [Understanding Licenses for the vGW Series on page 10](#)
 - [Obtaining, Installing, and Managing vGW Series Licenses on page 11](#)
 - Appliance Status—This area displays the version and last update information for the vGW Security Design VM. See “System Updates” on page 76 for more information on initiating an update.
- Related Documentation**
- [Understanding vGW Series](#)
 - [Understanding the vGW Series Settings Module on page 3](#)

Understanding Licenses for the vGW Series

This topic contains the following sections:

- [License Requirements on page 10](#)
- [vGW Series Licenses on page 10](#)
- [Evaluation Licenses on page 11](#)

License Requirements

To enable the vGW Series, you must:

- Purchase a license for the vGW Security Design VM and separate licenses for its features, if required.
- Obtain entitlement license keys for the licenses.
- Install the vGW Series components and features license keys, as required, and manage them.

The presence of an entitlement license key determines whether you can use a feature. For information about how to purchase software licenses for vGW Series features, contact your Juniper Networks sales representative.

vGW Series Licenses

You can purchase licenses for the following vGW Series components:

- vGW Security Design VM—You must purchase a license for the vGW Security Design VM. This component serves as the management center for the vGW Series.
- Each ESX/ESXi host has a physical CPU socket count. For each host that you want to protect, you must purchase separate licenses equivalent in number to its CPU sockets. This requirement applies to the following components and features:
 - vGW Security VM—A vGW Security VM helps secure and monitor the ESX/ESXi host that it runs on, and it reports information back to the vGW Security Design VM.
 - High-availability (HA)—Allows for the deployment of primary and secondary vGW Security VMs and vGW Security Design VMs to maintain solution resiliency in the event of any single component failure.

- **AniViVirus**—Protects VMs by detecting malware, identifying affected VMs, and allowing you to define a remediation plan. The vGW AntiVirus feature does this with minimal impact to performance and resources by centralizing scanning on the vGW Security VM and, when required, using a minimal agent, called an EndPoint, on each VM.
- **Intrusion Detection System (IDS)**—Allows you to examine virtual network traffic for malicious content or activity, for example, web attacks and distributed denial of service (DDOS) attacks.

Starting with two licenses, the number of licenses that you can purchase increases incrementally, depending on the license package. For Security VMs, HA, and IDS, and AntiVirus, licenses come in packages of 2, 10, 20, and upwards. You can also purchase a license for unlimited CPU sockets for each feature.

For all features except IDS and AntiVirus, licenses are perpetual. For IDS and AntiVirus, licenses are subscription-based. You can purchase a license for one year or for three years.

Evaluation Licenses

You can use an evaluation license to explore vGW Series product. The evaluation product is fully functional, and it has an embedded thirty-day license. The evaluation license enables you to use all vGW Series features. If you require a longer term license, contact your sales representative.

Related Documentation

- *Understanding vGW Series*
- [Understanding the vGW Series Settings Module on page 3](#)
- *vGW Series Prerequisites and Resource Requirements for the VMware Environment*

Obtaining, Installing, and Managing vGW Series Licenses

After you power-on the vGW Security Design VM, you run the vGW Series installation wizard. During this process, you are prompted for product license information. If you purchased the vGW Series, you enter the license key for the vGW Security Design VM. After you install the license key, a serial number is presented. You can use the serial number for product support.

For each component and feature that you want to use that requires a license, you must install an entitlement license key using the vGW Security Design VM. If the proper license keys do not exist, you cannot activate the feature or install an update.

You enter license keys in the Application Settings section of the Settings module. You use the Status & License section. You install and manage licenses in the Product Licensing section. You can also use this section to view existing licenses.

Related Documentation

- *Understanding vGW Series*
- [Understanding the vGW Series Settings Module on page 3](#)

CHAPTER 4

Installation

- [Configuring vGW Series Installation Settings on page 13](#)
- [Installing vGW Security VMs on ESX/ESXi Hosts on page 15](#)
- [Understanding vGW Series Timeout Parameters and the vGW Security VM Installation, Uninstallation, and Update Tasks on page 21](#)
- [Securing and Unsecuring Virtual Machines Using the vGW Security Design VM on page 22](#)
- [Understanding Automatic Securing of VMs on page 23](#)
- [Understanding the VMware Auto Deploy Feature for ESXi Servers and vGW Series Integration With It on page 25](#)
- [Configuring VMware Auto Deploy and vGW Series to Automatically Secure ESXi Hosts Provisioned by Auto Deploy on page 26](#)
- [Disabling the vGW Series Suspend-Resume Process Enacted After a VM Is Unsecured on page 34](#)
- [Removing vGW Security VMs from ESX/ESXi Hosts on page 36](#)
- [Integrating the vGW Series with VMware Using the Settings Module on page 37](#)
- [Understanding vGW Series Integration with vCloud Director on page 41](#)
- [Configuring vGW Series Integration with vCloud Director on page 43](#)

Configuring vGW Series Installation Settings

This topic covers installation settings that you configure using the vGW Security Design VM. You use the Install Settings section of the Settings module for this purpose. The Install Settings page contains the following panes:

- VMsafe installation
- Automatic Securing of VMs
- Policy per vNIC

In the VMsafe installation pane, you can:

- Select the vGW Security VM template to use to instantiate vGW Security VMs on ESX/ESXi hosts.

From the VMsafe Template list, select the template to use.

- Specify the security behavior to follow when a vGW Security VM is unable to attach to the vGW Series VMsafe kernel module or retrieve firewall policy from the vGW Security Design VM:
 - Allow traffic to and from the vGW Security VM without security controls enforced.
 - Stop all traffic to and from the vGW Security VM. In this case, VMware disconnects the VM's vNICs.
- Specify that the vGW Security VM should only monitor the activity of the VM, but not secure it.

In this case firewall policies are not loaded onto the vGW Security VM. Monitoring mode allows you to deploy a vGW Security VM without concern that security policies will block traffic.

- Automatically secure VMs. Specify the VMs in a particular group, VMs in a policy group or with a policy applied to them, all VMs, or no VMs to be automatically secured. For details see, [“Understanding Automatic Securing of VMs” on page 23](#).

For details on installing a vGW Security VM on an ESX , see [“Installing vGW Security VMs on ESX/ESXi Hosts” on page 15](#).

If you enable the Auto-Secure feature, it automatically secures VMs and attaches security policies to them. If you choose to secure VMs automatically, you have the option of excluding a group within the selected group from being automatically secured.

For details on securing VMs or removing them from a secured network manually, see [“Securing and Unsecuring Virtual Machines Using the vGW Security Design VM” on page 22](#).

You can configure information that allows you to assign separate policies to individual vNICs.

- You use the Policy per vNIC pane to specify:
 - Whether separate policies can be configured for individual vNICs on the same VM.
 - If one or more vNICs on a VM that is configured for Policy per vNIC can be exempted from having a security policy. That is, no security policy is attached to them and they are not secured by vGW Series.

You can use Policy per vNIC to apply policy rules to a vNIC that passes both IPv4 and IPv6 traffic.

For details on the Policy per vNIC feature, see [“Configuring the vGW Series Policy per vNIC Feature” on page 50](#).

For a VM with multiple vNICs, the Policy per vNIC feature allows you to use different policies for each of the vNICs. Users with VMs that connect to more than one port

group/vSwitch may want different policies for each of the networks that their VMs connect to. The Policy per vNIC optional parameter, SecurePervNIC, allows you to secure some of a VM's vNICs while leaving other of its vNICs unsecured. In this case, it is the VM/port group that you secure. That is, you can use different policies for a VM based on the VM/port group. To use SecurePervNIC, you must enable Policy Per vNIC. When you use SecurePervNIC, the actual distinction is the port group, not the vNIC. That is, the vNICs of a VM are secured per VM and port group. This is due to the ambiguity of having both a secured and unsecured connection to the same Port Group. To use SecurePervNIC, you must enable Policy Per vNIC.

Related Documentation

- *Understanding vGW Series*
- *Understanding the vGW Security VM*
- *Understanding the vGW Security Design VM*

Installing vGW Security VMs on ESX/ESXi Hosts

A vGW Security VM protects and secures virtual machines (VMs) on an ESX/ESXi host where it is installed. The vGW Security VM acts as a conduit to the vGW kernel module which it inserts into the hypervisor of the host that it protects when it is installed. The vGW Security Design VM pushes the appropriate security policy to the vGW Security VM which in turn inserts it into the vGW kernel module. All connections are processed and firewall security is enforced in the vGW Series kernel module. In other words, virtualized network traffic is secured and analyzed against the security policy in the vGW kernel module.

You deploy a vGW Security VM to each ESX/ESXi host in your environment that you want vGW Series to secure and monitor. The vGW Security VM protects VMs on that host and it gathers information about network traffic. It also maintains policy and logging information.

Securing an ESX/ESXi host with a vGW Security VM entails the following two parts:

- First you must install a vGW Security VM on the ESX/ESXi host to be secured. It is during this process that the vGW Security VM inserts the kernel module into the hypervisor of the ESX/ESXi host. This topic covers that process.
- Next you must select the VMs on the secured host that you want vGW Series to protect with a firewall policy and other features. The vGW Security VM obtains the policy for the VM from the vGW Security Design VM and provides the vGW Series kernel (hypervisor) module with it.

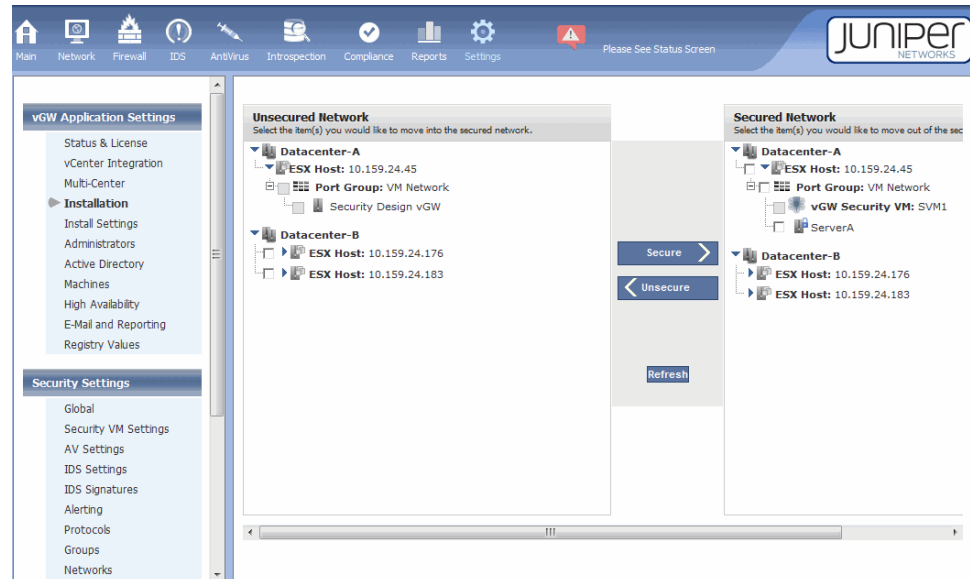
See [“Securing and Unsecuring Virtual Machines Using the vGW Security Design VM” on page 22](#) for details on the second part of the process.

To install the vGW Security VM on an ESX/ESXi host:

1. Select the Settings module **vGW Application Settings > Installation** page.
2. In the **Unsecured Network** pane, select the host in the data center that you want to secure with vGW Series. See [Figure 2 on page 16](#).

You can secure only one host at a time.

Figure 2: Securing an ESX/ESXi Host With a vGW Security VM

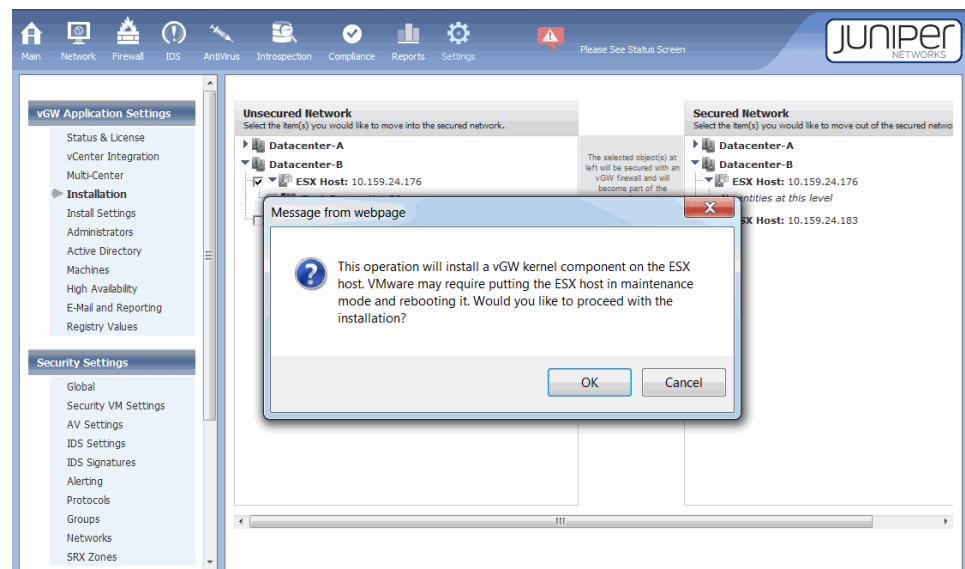


An empty check box appears before each host that is able to run the vGW Series kernel module. These hosts are not yet protected, but the check box indicates that you can secure them.

3. Click **Secure**.

After you initiate the installation process, a message is displayed indicating that VMware might require putting the ESX/ESXi host into maintenance mode and rebooting it. See [Figure 3 on page 17](#). Note that the message shown in this figure might differ somewhat depending on the vGW Series version that you are installing.

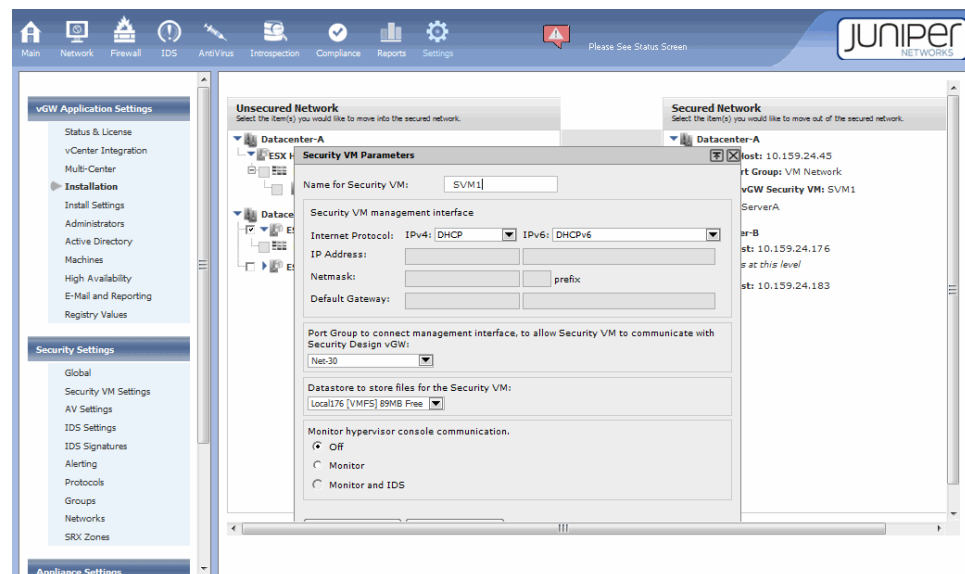
Figure 3: Installing a vGW Security VM on an ESX/ESXi Host



4. Click OK.

A dialog box is displayed allowing you to enter a name and specify other parameters for the vGW Security VM. See [Figure 4 on page 17](#).

Figure 4: Specifying vGW Security Parameters During Installation



Specify or select values for the following parameters:

- Enter a name for the vGW Security VM.
- Select the vGW Security VM security management interface addressing mode. The vGW Security Design VM communicates with the vGW Security VM

management interface based on this addressing mode. This interface must be reachable by the management interface of the vGW Security Design VM.

vGW Series supports both IPv4 and IPv6 address types. As such, the Installation Wizard for vGW Security VMs allows you to enter information for both types.

Select values for:

- IPv4
 - DHCP (Default): To obtain an IPv4 address, by default the vGW Security VM is configured to use DHCP. You do not need to specify additional information.
 - Static IP. If you select **Static IP**, you must specify a static IPv4 address and its network mask routing prefix, and the default gateway to assign to the vGW Security VM.
- IPv6
 - DHCPv6 (Default): To obtain an IPv6 address, by default the vGW Security VM is configured to use DHCPv6. You do not need to specify additional information.
 - Autoconfiguration. If you select **Autoconfiguration**, stateless address autoconfiguration is used to obtain the IPv6 address. It allows network devices attached to an IPv6 network to automatically acquire IP addresses and connect to the Internet without intermediate interaction with a DHCPv6 server.
 - Static IP. If you select **Static IP**, you must specify a static IPv6 address, including the IPv6 address prefix (the initial bits of the address that denote the network address, akin to a netmask), and the default gateway to use for it.

By default, a dual stack vGW Security Design VM communicates with a vGW Security VM using the IPv4 protocol. However, you can use the vGW CLI to change the default IP protocol used by setting the `center.dual.stack.default.communication.ipv4` parameter to false.

center.dual.stack.default.communication.ipv4=false

By default, this parameter is set to **true**. This parameter is relevant only if the vGW Security Design VM is configured for dual stack and one or more vGW Security VMs is also configured for dual stack. In all other cases, the protocol used is the one that is common to both the vGW Security Design VM and the vGW Security VM, and this parameter is irrelevant.

You can configure the vGW Security VM not to use dual stack in the following way:

- To use only IPv4 for vGW Security Design VM management communication with this vGW Security VM, disable IPv6. On the displayed list for the IPv6: box, select **Disabled**.
- To use only IPv6 for vGW Security Design VM management communication with this vGW Security VM, disable IPv4. On the displayed list for the IPv4: box, select **Disabled**.

How you configure addressing for the vGW Security VM affects its communication with the vGW Security Design VM management center. In an environment in which neither the vGW Security Design VM nor the vGW Security VM is configured for dual stack and the IP address types of their management interfaces are not the same, communication problems will occur. (For example, one interface might have an IPv6 address and the other might have an IPv4 address.) The vGW Security Design VM will not be able to connect to the vGW Security VM to carry out any procedures.

- c. Specify the port group to use to connect the vGW Security VM to the vGW Security Design VM.
- d. Specify the data store for the vGW Security VM.
- e. Specify if the hypervisor communication console should be monitored and if IDS should be used.

The dialog box allows you to enable console (hypervisor) monitoring *or* console monitoring and IDS.

- If you enable console monitoring, vGW Series monitors network traffic to the hypervisor console vNIC to ensure that inappropriate activity is not occurring.
- If you enable both console monitoring *and* IDS traffic monitoring, network traffic to the hypervisor console is monitored and IDS traffic is mirrored to the IDS engine.



WARNING: To use this option, you must first install an IDS license.

If at this point you do not enable console monitoring and IDS, you can do so later after you install a vGW Security VM. In that case, you use the Settings module Security Settings > Security VM Settings Network Monitoring tab and the IDS tab for a particular VM.

- f. Click **Secure**.

After you click **Secure**, the vGW Series associates all virtual NICs (vNICs) for the relevant VMs with the vGW Series kernel module.

VMware requires that the vNICs be disconnected and reconnected through a suspend and resume process. (VMs do not have access to the network during the few seconds that this process takes.) However, you can avoid the suspend and resume process by following the instructions covered in [“Disabling the vGW Series Suspend-Resume Process Enacted After a VM Is Unsecured” on page 34](#).

After you complete the installation, you might want to refine the configuration pertain to policy in the following ways:

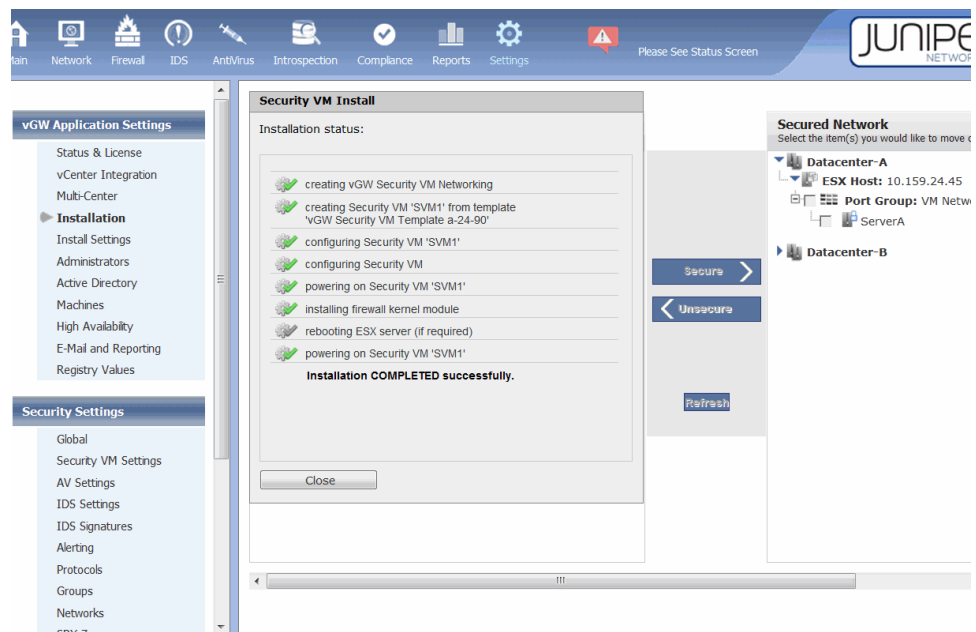
- By default, each vNIC has a restrictive default security policy. You can use the Firewall module’s Manage Policy tab to make the policy less restrictive.

- You can use the Policy per vNIC feature to configure separate firewall policies for individual vNICs on the same VM. For details on the feature, see [“Understanding the vGW Series Policy per vNIC Feature” on page 47](#) and [“Configuring the vGW Series Policy per vNIC Feature” on page 50](#).

After you define the vGW Security VM, vGW Series begins the vGW Security VM firewall installation on the selected host. It displays a progress report as it completes each task. If problems occur during the installation process, vGW Series displays messages describing them.

When the installation process is finished, vGW Series displays the list of completed tasks and the successful completion notice, as shown in [Figure 5 on page 20](#). Notice that in this case, as reported, it was not necessary to reboot the host.

Figure 5: vGW Security VM Installation Process Completion Notice



Related Documentation

- [Removing vGW Security VMs from ESX/ESXi Hosts on page 36](#)
- [Understanding the vGW Security VM](#)
- [Configuring Policy per vNIC to Secure Only Some of a VM's vNICs on page 55](#)
- [Installing a Secondary vGW Security VM for High Availability](#)
- [Updating vGW Security VMs in Batch Mode on page 137](#)
- [Understanding vGW Series](#)

Understanding vGW Series Timeout Parameters and the vGW Security VM Installation, Uninstallation, and Update Tasks

Configurations for the following two timeout parameters affect a variety of vGW Security VM installation, uninstallation, and update processes:

- `center.timeout.vm.long.in.sec` (default: 10 minutes [600 seconds])
- `center.timeout.host.long.in.sec` (default: 10 minutes [600 seconds])

These JunosV Firefly Host VM processes entail individual tasks and groups of tasks. For example, the JunosV Firefly Host Module removal process that occurs when a JunosV Firefly Host VM is being uninstalled includes the "enter maint(enance) mode" and "remove fastpath" tasks.

If the ESX/ESXi host on which the vGW Security VM was installed exceeded the configured timeout value while it was being put into maintenance mode during the vGW Security VM uninstallation, the message that vGW Series reported prior to vGW Series 5.5 might have been misleading because it pertained to the *group* of tasks comprising the kernel module removal process.

Beginning with vGW Series 5.5, when a task exceeds the configured timeout value that pertains to it, vGW Series generates a log error entry that describes the individual task that was being executed when the timeout event occurred and the timeout parameter configuration that controls it, rather than giving a single task group message.

For example, the following message is generated and written to the log when the process of cloning the vGW Security VM template exceeds the amount of time configured for `center.timeout.vm.long.in.sec`.

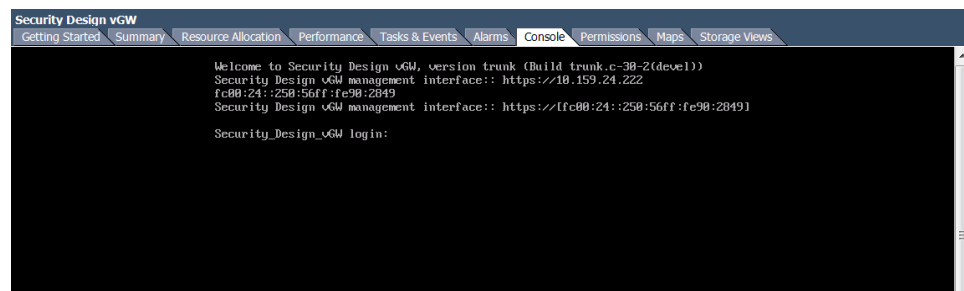
"Cancelled task (cloning Security VM X from template Y) as it was taking too long. Timeout set by center.timeout.vm.long.in.sec"

The timeout parameters are configurable to allow you to adapt your configuration to different vCenter behaviors. For example, a log entry might indicate that a vCenter task is taking longer than expected. You can use the console to run the vGW Series command-line interface (CLI) and change the configuration for the timeout parameter affecting the task. You can adjust the configuration appropriately and retry the process.

To use the vGW Series CLI from the vCenter console:

1. Launch the VMware vSphere Client.
2. Right-click the vGW Security Design VM icon on the left navigation panel to display a list of options.
3. Select the third option on the list, **Open Console**. Alternatively you can select the Console tab, as shown in [Figure 6 on page 22](#).

Figure 6: vGW Series CLI Console



The console window appears.

Some of the tasks affected by these timeout parameters are:

- vGW Security VM shutdown
- ESXi reboot
- cloning vGW Security VM template
- vGW Security VM reporting heartbeat with new version after update

Related Documentation

- [Installing vGW Security VMs on ESX/ESXi Hosts on page 15](#)
- [Removing vGW Security VMs from ESX/ESXi Hosts on page 36](#)
- [Installing a Secondary vGW Security VM for High Availability](#)
- [Updating the vGW Security Design VM on page 135](#)
- [Understanding the vGW Security VM](#)
- [Understanding vGW Series](#)

Securing and Unsecuring Virtual Machines Using the vGW Security Design VM

After you install the vGW Security VM on an ESX/ESXi host to secure it, the vGW Security Design VM allows you to manually secure virtual machines (VM) on that host or remove them from the protected network. Removing a secured VM from the protected network is referred to as *unsecuring* the VM.

To secure a VM that does not belong to the Secured Network:

1. In the vGW Security Design VM Settings module vGW Application Settings section, select **Installation**.
2. In the Unsecured Network pane, select the VM that you want to secure. Click the check box in front of its name.
3. Click **Secure**.

As it secures the VM, the vGW Series reports on the status of each part of the process. If the VM is successfully secured, the report states that the VM was successfully secured.

4. Click **Close**.

The vGW Security Design VM displays a process symbol that dynamically indicates that the VM is being secured with a firewall and moved into the secured network. The VM is now protected, and it appears in the Secured Network pane.

After all vGW Series components in your environment are upgraded to release 5.5, if you attempt to introduce components from a previous release, the process is halted and vGW Series displays a message informing you that you must install the correct version.

Related Documentation

- [Disabling the vGW Series Suspend-Resume Process Enacted After a VM Is Unsecured on page 34](#)
- [Installing vGW Security VMs on ESX/ESXi Hosts on page 15](#)
- [Understanding vGW Series](#)

Understanding Automatic Securing of VMs

vGW Series allows you to configure your system to *automatically* secure VMs. Auto-securing VMs streamlines policy application allowing you to efficiently ensure security throughout your virtual infrastructure. You can configure the Auto-Secure feature options to direct vGW Series to automatically secure VMs in the manner most appropriate for your environment.

You use the Settings module vGW Application Settings > Install Settings > Automatic Securing of VMs pane to configure Auto-Secure for your virtualized environment.

The Automatic Securing of VMs pane includes the following options:

- No VM

No individual VMs or groups of VMs are automatically secured. This is the default behavior.

- VMs in the following group

This option allows you to select either a Static Group or a Smart Group from the list of existing groups. The list contains all groups, including those configured as Policy Groups and those that are not. Using this option, you can select only one group.



NOTE: Only VMs in the selected group are automatically secured.

- If you did not configure the selected group as a Policy Group, vGW Series automatically secures members of the group with the Global and Default policies.

- If you configured the selected group with the Policy Group option, then any policy rules that were created for the group and applied to it take effect. In this case, the Default policy is not used.

- VMs with a VM Policy or in a Policy Group

Because Default Policy and Global Policy rules tend to be restrictive, they are not appropriate for securing all VMs. This option allows you to predefine policy rules for individual VMs and groups of VMs and direct vGW Series to use the policy rules that you predefined to automatically secure them rather than relying on just the Default and Global policy rules. Using this option, you can automatically secure many Policy Groups and individual VMs instead of being restricted to selecting a single group.

VMs that fit any of the following criteria are automatically secured:

- Individual VMs for which you have predefined specific policy rules and applied those policies using the Firewall module Apply Policy page to install the policy.
- Groups of VMs that you created as Static Groups or Smart Groups and for which you selected the Policy Group option. You must also have created and applied a policy for the group, and that policy must contain rules.

- All VMs

All VMs are automatically secured. As described previously, any policy rules defined for Policy Groups that have been previously applied take effect for VM members of the group. If a VM is not a member of any group, then Global and Default Policies and any individual VM rules take effect for them.

You can refine this selection by excluding a specific group of VMs.

- Optionally, exclude a group of VMs from being automatically secured. You might want to exclude VMs from auto-securing that you are using for testing.



NOTE: vGW Series auto-secure feature will not attempt to secure an FT-enabled VM. vGW generates an alert telling you that you must disable FT for that VM or suspend the VM for vGW to secure the VM. The auto-secure feature monitors for cases in which an FT-enabled VM is disabled and for VMs that are suspended and powered-off.

If a VM is automatically secured, you cannot use the Settings module Installation page to unsecure it. The VM is shown on this page in a dimmed box and a message is presented informing you that it is automatically secured. In this case, if you were able to unsecure the VM, vGW Series would simply secure it again automatically.

Instead, you must first remove the VM from the automatically secured group that it belongs to, or, if it is an individual VM, remove the policy from it, and then unsecure it.

Related Documentation

- *Understanding vGW Series*
- *Understanding the vGW Security VM*

Understanding the VMware Auto Deploy Feature for ESXi Servers and vGW Series Integration With It

vGW Series allows you to secure automatically ESXi hosts generated through the VMware Auto Deploy feature. This topic covers Auto Deploy and vGW Series automatic installation of vGW Security VMs for these hosts. It includes the following sections:

- [VMware Auto Deploy Feature on page 25](#)
- [vGW Series Support for Auto Deploy on page 25](#)
- [vGW Series Automatic Installation of vGW Security VMs on page 25](#)

VMware Auto Deploy Feature

Leveraging the network (PXE) boot capabilities of x86 servers, the VMware Auto Deploy feature allows a user to rapidly provision large numbers of ESXi hosts, efficiently and easily managing their hypervisor installation and upgrades. ESXi hosts that are deployed through Auto Deploy are automatically added to a host cluster. New hosts are provisioned based on user-defined specifications. The user can define specifications for various hypervisor images and host profiles to be used for different hosts.

After an ESXi host is network-booted from a central Auto Deploy server, a software image is installed on it and a vCenter host profile is then used to configure the host. When this process completes, the ESXi host is connected to vCenter and the user can create virtual machines (VMs) on it. Apart from defining rules governing images and profiles for collective use, this process is entirely automated allowing for quick provisioning without user intervention.

vGW Series Support for Auto Deploy

vGW Series is designed to work in tandem with the VMware Auto Deploy feature. It complements the VMware Auto Deploy feature by allowing you to automatically secure ESXi hosts. It is designed to work in tandem with the VMware Auto Deploy feature. You can configure it to automatically install vGW Security VMs on these hosts based on clusters that they belong to, on all ESXi hosts created through auto-deploy, or on none of them effectively disabling the feature.

vGW Series assigns a name to an automatically installed vGW Security VM based on a prefix that you specify (SVM Name prefix) when you configure vGW Series auto deploy support and an octet derived from the host's IP address.

vGW Series Automatic Installation of vGW Security VMs

vGW Series detects if an ESXi host has been added to the clusters that you selected when you configured vGW Series auto deploy support. For ESXi hosts in a selected cluster, it determines if a vGW Security VM is already installed on that host.

- If a vGW Security VM is already installed, vGW Series ensures that networking is set up to properly handle hosts that have been rebooted. (Restoring the network restores connectivity between the vGW Security VM and the fastpath.)

- If there is not a vGW Security VM installed on the host, vGW Series treats the ESXi host as one that was added to the cluster by the VMware Auto Deploy process. In this case, it follows the same process that it uses to install a vGW Security VM under normal conditions except for the following actions:
 - It verifies that the port group and the data store exist.
 - It omits the step that installs the fastpath module and the step that reboots the ESXi host because it is assumed the fastpath module was already embedded in the image that was deployed on the host.
 - If a failure occurs, it generates an alert. [Figure 7 on page 26](#) shows an example.

Figure 7: vGW Series Failure Alert for vGW Security VM Installation on Automatically Deployed ESXi Hosts

Priority	Date	Alert
H	05/14/13 10:45	firewall "svm_30" Kernel module status changed to ok
H	05/14/13 10:45	firewall "svm_30" vf fpstatus changed to ok
M	05/14/13 10:43	AutoStart option is turned off on some hosts. Host(s): 10.10.10.30, more
H	05/14/13 10:41	firewall "svm_30" power state changed to powered on
H	05/14/13 10:36	Auto Deploy SVM install failed on host 10.10.10.32, details: HostCommunication
H	05/14/13 10:35	Auto Deploy SVM install failed on host 10.10.10.31, details: HostCommunication
H	05/14/13 10:12	firewall "svm_32" Communication status changed from never communicated to communicating
H	05/14/13 10:12	firewall "svm_32" svm config changed to ok (Security VM configuration is ok)
H	05/14/13 10:12	firewall "svm_32" Time synchronization status changed to time synced
H	05/14/13 10:12	firewall "svm_32" High Availability status changed to active

Related Documentation

- [Installing vGW Security VMs on ESX/ESXi Hosts on page 15](#)
- [Understanding the vGW Security VM](#)
- [Understanding the vGW Security Design VM](#)
- [Understanding the VMware Infrastructure and vGW Series](#)
- [Understanding vGW Series](#)

Configuring VMware Auto Deploy and vGW Series to Automatically Secure ESXi Hosts Provisioned by Auto Deploy

You can configure vGW Series to monitor clusters for ESXi hosts that are provisioned through VMware's Auto Deploy feature and install vGW Security VMs on them automatically.

Before this topic explains how to configure vGW Series Auto Deploy support, the topic covers how to set up VMware for Auto Deploy.

- [Configuring Auto Deploy in VMware on page 27](#)
- [Configuring vGW Series to Support Auto Deploy on page 31](#)

Configuring Auto Deploy in VMware

This section provides procedures that cover how to set up VMware for Auto Deploy which allows you to deploy ESXi 5.0 hosts and their associated configurations automatically. If you encounter problems, please refer to the VMware documentation.

To set up Auto Deploy, you install a vCenter server, a vSphere client, the Auto Deploy service, a DHCP server, a TFTP server, and the Image Builder PowerCLI and Powershell. The Image Builder PowerCLI Powershell is a commandlet and scripting language that allows you to build ESXi-based images and create rules to push out those images to your ESXi hosts.

This process requires virtual machines (VMs) for the following components and it requires the specified connectivity.

Prerequisites:

- VMs. You must create VMs to be used for:
 - VMware vCenter.
 - VMware Auto Deploy.



NOTE:

VMware recommends that you install the Auto Deploy service on the same VM as vCenter.

- VMware vSphere to run PowerCLI, which requires PowerShell.
- A DHCP server.
- A TFTP server.
- There must be at least one ESXi host whose MAC address you know.
- You must have control over IP assignment on the network.

The following procedure explains how to install the Auto Deploy service and the components it relies on. It also covers how to create an Auto Deploy image profile using PowerCLI.

1. Install vCenter server 5.0, if it is not already installed.
2. Install the vSphere 5.0 client, if it is not already installed.
3. Install the Auto Deploy service.

The Auto Deploy service is a Web server that serves up ESXi images. The Auto Deploy service is embedded in the vCenter server appliance (vApp). When you install that appliance, Auto Deploy is automatically configured.

However, to completely configure Auto Deploy you specify the location for the repository where the ESXi images are stored and the repository size. You also configure

an Auto Deploy connection to the vCenter server, and you specify the IP address that the Auto Deploy service should use to communicate with the network.

To verify that the Auto Deploy service is connected and configured, in vSphere, click **Home > vCenter Service Status**.

4. Install a TFTP server.

A TFTP server is required to push the boot loader to the ESXi host. You can install it wherever you choose, including on the same VM as the vCenter server.

After you complete this process, the TFTP folder contains the boot loader that is streamed to the ESXi host.



NOTE: Ensure that access to the TFTP server is granted. Also, disable IE ESC in MS Windows. If it is not disabled, error messages are generated reporting that you do not have access permission.

You can install any TFTP server, for example, SolarWinds or Open TFTP. In any case, ensure that the timeout settings allow sufficient time to boot at least 4 ESXi hosts concurrently.

a. In vCenter, at Home > Administration > Auto Deploy, click **Download TFTP Boot Zip**.

b. Download the ZIP file and extract the contents to the root folder on the TFTP server.

c. Configure the TFTP server and start the server instance.

Ensure that the ESXi host is able to access it—that is, that no firewall rules are configured that would prohibit access.

5. Install the Image Builder PowerCLI and Powershell.

You enter all commands called out in this section in the PowerCLI.

a. Change the execution policy. Enter the following command:

set-executionpolicy remotesigned

6. Get the required images.

- Download the ESXi software depot (repository).

This is not the ISO image. Rather, it is a file that VMware provides that has a name similar to the following one:

VMware-ESXi-5.0.0-469512-depot.zip

- Get the vGW Series VIB ZIP file.

There are no restrictions on where you download this to.

7. Using PowerCLI, create the Auto Deploy image profile and add the ESXi image to it.

The image profile contains all module and features that you want to bundled together.

Note that for all ZIP files, the command must include the filename with the .zip extension.

- a. Connect to vCenter.

If you installed PowerCLI on vCenter, at the command line enter:

connect-viserver localhost

- b. Add the ESXi depot. Enter the following command:

add-esxsoftwaredepot ESXi-depot-zip-full-path

- c. Add the vGW Series VIB ZIP file. Enter the following command:

add-esxsoftwaredepot VIB-zip-full-path

Specify for the full path to where you downloaded the VIP ZIP previously, include the ZIP file name.

- d. Create an ESXi image profile and add the ESXi image to it. Enter the following command:

new-esximageprofile -cloneprofile "VMware-ESXi-5.0.0-469512-standard" -name "image-profile-name"

The **new-esximageprofile** command clones an existing profile whose name you specify as the value of the (**-cloneprofile**) argument. The source image profile name is derived from the name of the ESXi software depot. It follows the version number of the depot file that you retrieved previously, for example **"VMware-ESXi-5.0.0-469512-standard"**.

It could happen that the value that you specify for **-cloneprofile** causes an error to be generated, for example, because the VMware naming scheme has been changed. In this case, you can retrieve a list of profiles to find the correct name of the profile to clone. The name should have the same 6-digit build number as that of the depot ZIP file.

To get a list of profile names, enter the following command:

"Get-EsxImageProfile?"

You can specify any name for the image profile **"image-profile-name"** to be created from the original one.

- e. Add the vGW Series VIB to the image profile. Enter the following command:

add-esxsoftwarepackage -imageprofile "image-profile-name" --softwarepackage dvfilter-altor-vf

To obtain the software package names, enter the following command:

get-esxsoftwarepackage

- f. Create a deploy rule. The deploy rule downloads and installs all of the modules for the image into the Auto Deploy repository.

Enter the following command:

```
new-deployrule -name "auto-deploy-rule-name?" -item "image-profile-name?"
-AllHosts?
```

- Specify the name of the image profile that you created previously.
- Specify a name for the deploy rule that you are adding to the image profile ("auto-deploy-rule-name").



NOTE: The rules specifies that the image applies to all hosts (-AllHosts?).

- g. Create an image profile ZIP file and export it to where you want the file to reside. Enter the following command.

```
export-esximageprofile -imageprofile "image-profile-name?" -exporttobundle
-filepath image-profile-location-full-pathname.
```



WARNING: Consider that PowerCLI is session based. If you exit the PowerCLI session without first exporting the bundle to the repository, the image cannot be reused.

- h. Add the deploy rule that you created. Enter the following command:

```
add-deployrule -deployrule "auto-deploy-rule-name?"
```

8. Set up DHCP to network-boot the ESXi host:

- Get the MAC address of the ESXi host.
- On the DHCP server:
 - Create an IP reservation for the ESXi host using its MAC address.
 - Add option 66 (Boot Server Host Name - TFTP server IP).
 - Add option 67 (Bootfile Name - undionly.kpxe.vmw-hardwired).

9. Boot the ESXi host.



NOTE: The ESXi host should appear in a vCenter datacenter automatically.

Verify that the vGW VIB was installed. Select the ESXi host, click the **Hardware Status** tab, and expand **Software Components**. You should see the following entry: dvfilter-altor-vf.

- After your ESXi host is booted, some components will not have been set up. To resolve this, you can create a host profile and set it to the cluster where your hosts will be booted.

Before you create the host profile, set up the following components:

- network and storage.
- additional NICs.

After you create the host profile, configure the administrator password (Security configuration > Administrator password).

If you have multiple clusters, new ESXi hosts are placed through Auto Deploy in any available ones. To direct new ESXi hosts to a specific cluster, create a separate deploy rule using the following command. For example:

```
New-DeployRule -name "HostCluster" -item cluster-name -Pattern
"ipv4=10.70.1.1-10.70.1.250"
```

```
Add-DeployRule -DeployRule HostCluster
```

Configuring vGW Series to Support Auto Deploy

Prerequisites

For vGW Series to automatically install vGW Security VMs on ESXi hosts provisioned by VMware Auto Deploy:

- A version of the fastpath driver that vGW Series would have installed if you had installed the vGW Security VM using the installation process.
- The `net.dvfilterbindipaddress` (Net.DVFilterBindIpAddress) value must be set to 169.254.65.1. Use VMware to set this property yourself. The vGW Security Design VM will set it during the installation process. However, it is better to set it in VMware.

To navigate to the location where you can set the `net.dvfilterbindipaddress` host property, in vSphere on the ESXi host, select **Configuration** > **Software**, and click **Advanced Settings**.

- Create a vSwitch to contain port groups for both the fastpath driver and the vGW Security VMs.

The vSphere Client Add Network wizard guides you through processes that allow you to create a virtual network to which VMs connect, including how to create a vSwitch. You can also create a vSwitch using the vSphere Configuration > Networking > Virtual Switch view for the selected ESXi host. You can add or modify a VM port group using the vSphere client. The vSwitch for vGW Series Auto Deploy support has two port groups, one for the fastpath driver and another for vGW Security VM.

You must use `vmervice-vswitch` as the name for the vSwitch.

- For the fastpath driver, you must use `vmervice-vmknic-pg` as the name for its port group.
- There are no guidelines or requirements imposed on naming the port group used for the vGW Security VM. Normally this name is generated by the vGW Security Design

Center based on the vGW Security VM ID. Because the vGW Security VM does not yet exist, this information is unavailable.



NOTE: The purpose of using a unique name for the vGW Security VM port group is to obstruct vMotion movement of that vGW Security VM away from the ESXi host that it is installed on. However, if the vGW Security VM were to be moved from its ESXi host, the vGW Security Design VM would detect it and, using vMotion, it would move it back. For that reason, a unique name is not essential.

You use the Automatic Securing of Auto-deployed hosts pane of the Settings > vGW Application Settings > Install Settings page to configure vGW Series to automatically secure these hosts. See [Figure 8 on page 32](#).

vGW Series automatically installs a vGW Security VM on the selected hosts.

Figure 8: Configuring Automatic Installation of vGW Security VMs for Auto-Deployed ESXi Hosts

Automatic Securing of Auto-deployed Hosts

Select which auto-deployed hosts you would like to auto-secure

☐ No Host
☐ All Hosts
☒ Hosts in the following clusters:

☒ cluster_a
☒ cluster_b
☐ cluster_c2lk

The Security VM will be automatically named, using a prefix string you supply appended with the last octet of its corresponding ESX Host IP address, in the form of [prefix].[octet].

SVM Name prefix: Example: SVM_123
 Port Group:
 Datastore:

Security VM IP address assignment. A static address will be created from the provided subnet followed by the last octet of the ESX IP address.

Method:
 IP Address: . XXX
 Network Mask:
 Default Gateway:

☐ Force recheck on all hosts

Save

To configure vGW Series to install a vGW Security VM on selected ESXi hosts that are automatically deployed:

1. Select the ESXi hosts to secure:
 - **No hosts:** No hosts will be secured.
 - **All hosts:** All hosts will be secured.
 - **Hosts in the following clusters:** Only hosts in the clusters that you identify will be secured. Select the check box for each cluster that you want to include.
2. Specify a prefix to use as part of the name that is assigned to every automatically installed vGW Security VM. Select the port group and the data store to use.
 - **SVM Name prefix**—vGW Series automatically assigns a name to a vGW Security VM. It uses this value as the prefix. To create the complete name, the value is prepended to the last octet of the ESXi host IP address in the format `[prefix]_[octet]`.
 For example, if you used SVM_ as the prefix, if the last octet of the ESXi host IP address to be secured was 123, the name SVM_123 would be assigned to the vGW Security VM for that host.
 - **Port Group**—From the **Port Group** list, select the network label for the port groups.
 Port groups serve as anchor points for VMs that connect to labeled networks. A port group is identified by a unique network label. The same network label is used for all port groups in a datacenter that are physically connected to the same network.
 When you select either All Hosts or specific clusters, vGW Series updates the port group selection list. However, the list includes only port groups that are common to *all* connected hosts.
 This behavior applies if you select one cluster or more than one.
 - **Datastore**—From the **Datastore** list, select the datastore to use for the vGW Security VMs.
 When you select either All Hosts or specific clusters whose hosts are to be secured, vGW Series updates the datastore list to include their datastores. The list includes only options that are common to *all* connected hosts. If there are no datastores that are on *all* hosts, the list is empty. However, if there is only one connected host, the list will show all of the datastores that are on that host.
 This behavior applies to all clusters, whether you select one or more.
3. On the Method list, select the method to use to acquire IP addresses for the vGW Security VMs.
 - **Method**—Select either DHCP or static.
 - **IP Address**—If Method is set to static, specify the static IP address to assign to the vGW Security VM.

- **Network Mask**—Specify the network mask to use in the IP address for the vGW Security VM.
 - **Default Gateway**—Specify the default gateway for the vGW Security VMs.
4. To override the limit restricting the number of times that vGW Series is allowed to attempt to install vGW Security VM on a host after repeated failures, reset the error count. Select **Force recheck on all hosts**.

vGW Series maintains a count of the number of failed attempts for each host. When that count is exceeded, it no longer tries to install a vGW Security VM on it. The installation attempts limit is set in the **center.auto.deploy.svm.install.retry.count** parameter which has a default of 3 times. If you select this check box, the count is reset. It is also reset if you modify configuration settings.

You can create a per-host XML configuration. If you do this, the file must reside at `/usr/lib/tomcat/webapps/ROOT/WEB-INF/autoDeploy.xml`. You can find the xsd to use at:
<http://vgw-milford.juniper.net/trac/browser/center/branches/fullers/schemas/autoDeploy.xsd>.

The fallback behavior is:

- If the static IP and IP or netmask or gateway are not set, configuration information set in the vGW Security Design VM is used.

For example, if you set the IP method to DHCP in the vGW Security Design VM and a per-host configuration host entry does not have the IP configuration method specified, then the vGW Security VM for that host would get DHCP.

- If the port group or data store are not found, the installation is cancelled and a message is issued in the error log.

Disabling the vGW Series Suspend-Resume Process Enacted After a VM Is Unsecured

You use the vGW Security Design VM Settings module Installation section to secure and unsecure a VM. By default, the vGW Series suspends and resumes a VM when you unsecure it. You can change this behavior by changing the value of the `vm-safe.config` option.

- [Displaying the State of the vm-safe config Setting on page 34](#)
- [Disabling the Suspend-Resume Process on page 35](#)

Displaying the State of the vm-safe config Setting

This example shows the default setting. You can use the following command to display the current state of the `center.config vm-safe config` option:

```
(Cmd) config show center.suspend.after.vmsafe.config
# whether center should suspend and resume VM after VMsafe configuration
center.suspend.after.vmsafe.config = true
```


Disabling the Suspend-Resume Process

In some cases it might be necessary or desirable to stop vGW Series from enacting the suspend-resume process after a VM is unsecured. For example, you might want to disable the process to allow the VM to be migrated to another host or to suspend and resume the VM later after completing the removal of protection from the VM.



TIP: Take care when you protect VMs such as the VMware vCenter Database VM and other VMs that must not be suspended.

To enable the vmsafe config process to take effect after the VM is migrated to another host without suspending the VM, use the following statement. Set the option to false in center.config:

```
(Cmd) config set center.suspend.after.vmsafe.config false
```

After changing this value, either restart the vGW management process or reboot the vGW Security Design VM. You can use the service restart command line or the vGW Security Design VM to restart the vGW management process.

To restart the vGW management process from the command line, enter the following command:

```
(Cmd) service restart tomcat
Sending 'restart' command
The following watches were affected:
tomcat
```

To restart the vGW management process using the vGW Security Design VM:

1. Select the Settings module Support section.
2. In the Restart pane of the displayed page, click **Restart**.

Related Documentation

- [Installing vGW Security VMs on ESX/ESXi Hosts on page 15](#)
- [Securing and Unsecuring Virtual Machines Using the vGW Security Design VM on page 22](#)
- [Understanding vGW Series](#)

Removing vGW Security VMs from ESX/ESXi Hosts

This topic explains how to remove a vGW Security VM from an ESX or an ESXi host.

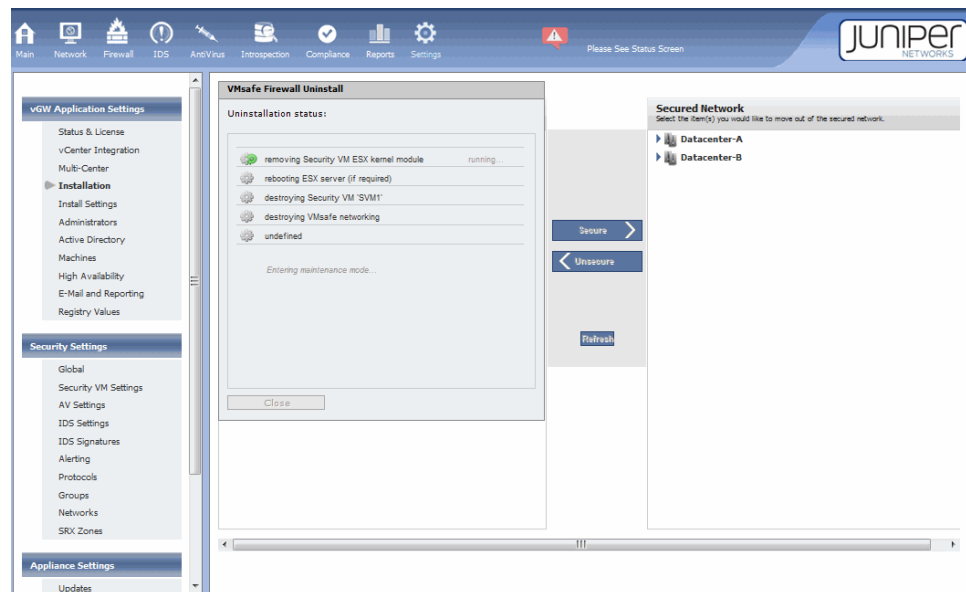
If you want to remove the VMX entries before you un-install the vGW Security VM, then before unsecuring the entire host by removing the vGW Security VM, unsecure the individual VMs. See [“Securing and Unsecuring Virtual Machines Using the vGW Security Design VM”](#) on page 22.

To un-install the vGW Security VM from a host:

1. In the Secured Network pane of the Settings module vGW Application Settings > Installation page, select the host that you want to move out of the secured network.
2. Click the **Unsecure** arrow button.
3. The VMsafe Firewall Uninstall status pane is displayed. As the vGW Security Design VM removes the firewall from the host—or moves a specific VM out of the secured network, if you selected a VM—the status pane identifies the active process.

When you select an individual VM to remove from the secured network and click **Unsecure**, the vGW Security Design VM removes all relevant VMX entries for that VM, reverting the VM to its state prior to vGW Series protection of it. [Figure 9 on page 36](#)

Figure 9: vGW Security VM Uninstall



If you plan to un-install vGW Series from your virtualized environment, unsecure all VMs in this manner. Afterward, select the check box for each of the ESX/ESXi hosts and click **Unsecure** to remove them from vGW Series protection. This process removes the kernel module and the related VMservice vSwitch and port groups.

Unsecuring a host before removing its VMs does not affect the VMs adversely. However, the process does not remove VMsafe VMX entries that pertain to vGW Series. These entries are no longer required by that VM.



NOTE: You might not want the VMX entries for a VM to be removed under these conditions. For example, you might want to remove only the vGW Series kernel module from a specific host. This might be the case if you want the VMs to be moved to a different ESX/ESXi host for protection, or you intend to reinstall vGW Series later.

**Related
Documentation**

- [Installing vGW Security VMs on ESX/ESXi Hosts on page 15](#)
- [Understanding vGW Series](#)

Integrating the vGW Series with VMware Using the Settings Module

This topic explains the vCenter Integration settings page that allows you to configure parameters that control the interaction between vGW Series and VMware. It covers how to change the vGW Series VMware settings, direct VMware to update the vGW Security Design VM with VMs inventory information, change the settings that control how deleted VMs and information about them is handled, and how to integrate the vGW Series with the VMware infrastructure.

You can also use it to change the management domain, or scope, for the vGW Security Design VM, after you configure it initially when you install the product. The management domain specifies the data centers and host clusters in the vCenter that your vGW Security Design VM manages.

The vGW Security Design VM uses the VMware Virtual Infrastructure APIs to:

- Obtain VM Inventory information
- Determine resource utilization status
- Determine events affecting the VMs

The account used for vCenter must have read-write access to the VMware Infrastructure. You can use a custom account created in VMware; this approach makes it easier to identify and monitor activities that change. In any case, the account must have administrator privileges.

The Settings module vGW Application Settings > vCenter Integration page contains the following panes and their settings for which you either enter information or whose values you can change:

- **vCenter Settings**—Login information required for the vGW Security Design VM to communicate with the VMware vCenter and for administrator access to the vCenter. Specify the following information:
 - **Server Name or IP Address:**—Name of the vCenter or its IPv4 or IPv6 address.

- **Username:** and **Password:**—Your administrator authentication information for accessing vCenter.
- **Scope**—Allows you to specify the vCenter's data centers and host clusters to be managed by your vGW Security Design VM. You set this value initially when you install the product. See *Setting Up vGW Series* for details on initially setting the management domain.

You use this pane to change the management domain scope. The scope for your vGW Security Design VM can be:

- **Entire vCenter**—In this case, the vGW Security Design VM is able to access and manage all VMs and other entities in all data centers in the vCenter.

To use this scope, select **Entire vCenter**.

- **Datacenter**—A subset of data centers in the vCenter.

In this case, the vGW Security Design VM is able to access and manage only the VMs and other entities in the selected data centers.

To use this scope:

1. Select **Datacenters**.

vGW Series displays all of the vCenter's data centers.



NOTE: To update the list of data centers at any time to show changes—datacenters that might have been added or removed—click **Refresh**.

2. Select the data centers for your vGW Security Design VM to manage.

Ensure that each data center is assigned to only one vGW Security Design VM. Otherwise, unexpected consequences can occur.

For an overview of the Split-Center feature, see [“Understanding the vGW Series Split-Center Feature” on page 59](#).

3. Click **Save**.

- **Clusters**—A subset of host clusters in a data center. In this case, the vGW Security Design VM is able to access only the VMs and other entities on the selected host clusters.



NOTE: All of the host clusters that you select to belong to a management domain (scope) must be in the *same* data center. You can not include host clusters from two or more different data centers in the scope.

To use the Clusters scope:

1. Click **Clusters** in the *Select a scope for your Security Design vGW* area.
In response, vGW Series displays a list of available data centers.
2. Select a data center from the displayed list whose host clusters you want the vGW Security Design VM to manage.
 - a. Click the arrow at the end of the box beside **Datacenter**: to display a list of data centers for the vCenter.
 - b. Click the data center whose cluster(s)/host(s) you want your vGW Security Design VM to manage.
vGW Series displays a list of cluster(s)/host(s) for the data center that you selected.
3. Select the check box before the names of the cluster(s)/host(s) that you want to include in your management domain.
4. Click **Save**.



NOTE: Ensure that each host cluster is assigned to only one vGW Security Design VM. Otherwise, unexpected consequences can occur.

You can change the cluster selection at any time. However, when you change the cluster scope, either of the following conditions can occur:

- Some vGW Security VMs could become unmanaged—This can occur when you remove a cluster from the list of selected clusters. Any vGW Security VM installed on an ESX/ESXi host that belongs to the removed cluster will no longer be accessible, and therefore it is no longer managed by the vGW Security VM.
- Some unmanaged vGW Security VMs could become accessible—If ESX/ESXi hosts that belong to a cluster that you add to your vGW Security Design VM management domain had a vGW Security VM installed on them by a different vGW Security Design VM, you could gain access to the vGW Security VMs. It is possible and important to gain access to an unmanaged vGW Security VM when you add its host cluster to your vGW Security VMs management domain for the following reason.

When a vGW Security VM becomes inaccessible because of cluster or datacenter selection changes its original vGW Security Design VM, its operational state might be compromised unless it is imported into another vGW Security Design vGW. This is because the vGW Security VM continues to try to communicate with its original vGW Security Design VM, which no longer recognizes it as a managed.

To view a list of unmanaged SVMs and render them manageable again:

1. Display the Settings module > Security VM Settings page.

The unmanaged vGW Security VMs are identified by a gray triangle status indicator.

2. To make a vGW Security VM manageable again, click its row to select it.
3. Click **Import**.

After you save the selection, vGW Series synchronizes all objects from vCenter. When it completes the process, vGW Series displays a message indicating the ESX/ESXi hosts and the VMs that were found.

- Deleted VMs and Groups—vGW Series can show information about any VMs and groups of VMs that it has encountered across time even if the VMs were deleted in VMware's vCenter system repository. This capability allows you to keep historic traffic records. It allows you to see all activity occurring in VMware across time. The VM's information persistency in the vGW Security Design VM can reveal attempts by a malicious administrator or hacker to bring up a VM, perform an unauthorized activity, and then delete the VM to hide their tracks.

You can change how vGW Series handles VMs that are deleted from vCenter using the following settings:

- **Hide deleted VMs from view in the Inventory Tree** check box.

By default, the "Hide deleted VMs from view in the Inventory Tree" check box is selected. However, if you do not want the deleted VMs appearing in the VM Tree, you can clear this menu item and they will be hidden from view.

The deleted VMs are still available to view again. By selecting the check box, they are again made visible in the VM Tree.

- **Delay before purging deleted VMs and Groups in days (-1 = never):** setting.

Enter the number of days after which vGW Series should purge deleted VMs and groups of VMs that have been deleted from vCenter. After that time, the VMs and all information pertaining to them is permanently deleted from vGW Series. For example, if you do not change the default value of 30 days and a VM is deleted in vCenter, at any time up to 30 days vGW Series is still able to make the VM information visible again (unhide). On the 31st day, the VM and all information pertaining to it is permanently removed from vGW Series.

- vGW Series management server plugin—Use this button to install the vGW Series plug-in into the vCenter interface.
 - To install the plug-in, click **Register**.
 - To view and use the plug-in, in the **vSphere Client interface** select **Home -> Solutions and Applications**.
 - To remove the vGW Series Management Plug-in, click **Unregister**.
- Automatic Startup of the vGW Security Design VM and Firewall—Use this setting to enable or disable the startup of vGW Series components when an ESX/ESXi system reboots. vGW Series components are set to start up automatically by default.

- Synchronize machine name—Changing the name of a VM in vCenter by default causes the name of the equivalent VM object in vGW Security Design VM to be changed to the same value. To override this setting, clear the value for this item.

For example, security administrators might want to use this override feature if they are not using the same naming convention as the VM team. The ability to override the default behavior is also useful if security administrators have created dynamic security policies using the name of the VM, and they do not want them affected by simple name changes in the vCenter.

**Related
Documentation**

- *Understanding vGW Series*
- *Understanding the VMware Infrastructure and vGW Series*
- *Understanding the vGW Security Design VM*
- *About the vGW Security Design VM Tree*

Understanding vGW Series Integration with vCloud Director

The vGW Security Design VM integrates directly with VMware's vCloud Director to allow vGW Series to retrieve information from vCloud Director about virtual machines (VMs). After you configure vCloud in the vGW Security Design VM, the information about a VM that it acquires can be used to dynamically associate that VM with vGW Series groups and policies that you create.

- [VMware vCloud Director on page 41](#)
- [vGW Series and vCloud on page 41](#)
- [Requirements on page 42](#)

VMware vCloud Director

VMware's vCloud Director Infrastructure-as-a-Service solution allows for rapid provisioning of complete virtual software-defined datacenter services. vCloud Director implements pooling, abstraction, and automation of data center services including storage and networking services. Using it, administrators can provision infrastructure without concern for physical hardware configuration.

Although vCloud Director can be used within an enterprise infrastructure, it is commonly used by cloud-based VM hosting providers.

vGW Series and vCloud

The vGW Security Design VM direct integration with vCloud Director allows it to collect information that is associated with a VM in vCloud Director. Information that vGW Series collects includes:

- VM membership in a specific organization.
- VM tags defined in the VM metadata. vCloud Director can associate information about VMs from its Metadata tab page that is configured by an administrator or other user, based on their permissions.

The vGW Security Design VM obtains the VM name and value data from this configuration. The vGW Security Design VM can obtain multiple values, if any.

vGW Security Design VM allows you to define Smart Groups used as policies in which VMs that match the Smart Group criteria are dynamically associated with the group, and its policy is applied to them. The vCloud Director information used in a dynamic group is associated with the `vcd.tag` property. The information appears as comma separated *attrname=value* pairs with the organization information appearing as the value for the `OrgName` attribute, such as `OrgName=Org1`.

For example, you could define a Firewall policy to be assigned to all VMs belonging to a particular organization. If the Smart Group configuration includes that organization, the Smart Group's policy is applied to the matching VM.

You might define an Introspection Image Enforcer profile that specifies that all VMs running Windows OS that belong to a particular organization must have installed on them all applications installed on a Gold Image that they are compared to. You could also use the information acquired from vCloud Director in configuring AnitVirus scanning.

vGW Series and vCloud Director integration is characterized as follows:

- By default, vGW Security Design VM integration with vCloud Director is disabled.

To enable integration with vCloud Director, you set the `center.vcd.enabled` parameter to true: **`center.vcd.enabled=true`**.

By default it is set to false.

- vGW Series supports integration with vCloud Director 5.1 and later versions.
- Presently the vGW Security Design VM supports integration with only one vCloud Director server.

Requirements

For vGW Security Design VM to be able to integrate with vCloud Director and query it for VM inventory and other operations, the account connecting to vCloud Director must have admin privileges.

Related Documentation

- [Configuring vGW Series Integration with vCloud Director on page 43](#)
- [vGW Series Attributes for VMware on page 118](#)
- [Understanding vGW Series Groups on page 111](#)
- [Creating vGW Series Smart Groups for VMware on page 114](#)
- [Understanding vGW Series](#)

Configuring vGW Series Integration with vCloud Director

This topic covers how to integrate vGW Series with VMware's vCloud Director using the vGW Security Design VM.

Before you configure vGW Series integration with vCloud Director, you must set up vCloud Director to send relevant notifications to an Advanced Message Queuing Protocol (AMQP) broker.

vCloud Director includes an AMQP service that you can configure to work with an AMQP broker to make available notifications about events in the cloud.

There are several AMQP-compatible brokers, including:

- Red Hat MRG Messaging. See <http://www.redhat.com/products/jbossenterprisemiddleware/messaging/>
- RabbitMQ. See <http://www.rabbitmq.com/>



NOTE: On the vCloud Director Administration Screen page that you use to configure the AMQP Broker settings, you must select **Enable Notifications**. Also, set **Exchange** to **vgwExchange**. If you use a different value, ensure that it matches the value of property `center.vcd.amqp.exchange` in `center.conf`.

After you complete this configuration and you configure the vGW Security Design VM for integration with vCloud Director, the vGW Security Design VM can register with the AMQP broker to acquire these notifications and use them for updates.

The Advanced Message Queuing Protocol (AMQP) is an OASIS open standard application layer protocol for message-oriented middleware. The defining features of AMQP are message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security.

To configure vGW Series integration with vCloud Director:

1. Enable vCloud Director integration. Set the `center.vcd.enabled` parameter to true:

`center.vcd.enabled=true`

By default it is set to false.

For this configuration parameter to take effect, you must restart Apache Tomcat.



NOTE: If you reset this value to false, all existing connections with vCloud Director are closed and the credentials are removed from the vGW Series database. Also the pane for configuring vCloud Director credentials in **Settings > vGW Application Settings > vCenter Integration** shown in [Figure 10 on page 44](#) is no longer displayed.

Figure 10: VGW Security Design VM vCenter Integration Window Showing vCloud Director Settings Pane

The screenshot displays the vGW Security Design VM vCenter Integration window. The left sidebar shows the navigation menu with 'vCenter Integration' selected. The main content area is divided into several panes:

- vCenter Settings:** Contains fields for 'Server Name or IP Address' (10.156.24.77), 'Username' (QA-SVC-Center), and 'Password'. It also has a 'Delete a scope for your Security Design vGW' section with radio buttons for 'Index vCenter', 'Datastore', and 'Cluster'. Below this is a 'Deleted VMs and Groups' section with a checkbox for 'Hide deleted VMs from view in the inventory tree' and a 'Delete before purging Deleted VMs and Groups in Data (14 days)' option. The 'Automatic Startup' section has a checkbox for 'Enable or disable automatic startup of the vGW management server and Security VM upon reboot of the host hardware'.
- Update VMs:** A section with a checkbox for 'Update IP addresses as they change in vCenter. If not selected, IP addresses will not be changed even they are inside network or not manually.' and an 'Update' button.
- vGW management server plugin:** A section with 'Register or unregister vCenter Client plugin' and 'Register vGW management server as a vCenter Client plugin' buttons.
- Synchronize machine name:** A section with a checkbox for 'Determine whether the machine name in the vGW management server is updated when VMs are imported in vCenter' and a 'Save' button.
- vCloud Director Settings:** A section with a 'Provide information to connect to the vCloud Director server' form. It includes fields for 'vCD Server Name or IP Address' (10.156.27.185), 'vCD Server Port' (443), 'vCD Username' (admin@vcd.com), and 'vCD Password'. Below this is a 'Provide information to connect to the AHQ server' form with fields for 'AHQ Server Name or IP Address' (10.156.27.146), 'AHQ Server Port' (8072), 'AHQ Username' (guest), and 'AHQ Password'.
- Synchronize vCloud Director data:** A section with a 'Restart vCloud Director synchronization process' button.

2. Figure 10 on page 44 shows the Settings > vGW Application Settings > vCenter Integration window that you use to configure vGW Series settings for integration with vCloud Director.

In the vCloud Director Settings pane, configure the following information:

- In the **VCD Server Name or IP Address** field, enter the IP address or DNS name of the vCloud Director server.

You can specify an IPv6 or IPv4 address.

- In the **VCD Server Port** field, if the port number differs from the default of 443, specify the port number.
- In the **vCD Username** field, enter the user type.

The user specified must have admin privileges.

- Specify a password in the **vCD Password** field

3. In the Synchronize vCloud Director pane, click **Restart**.

The vGW Security Design VM automatically configures information about any VM that it discovers through vCloud Director and it associates that information with the VM. You can view that information on the Settings > vGW Application Settings > Machines page.

- Related Documentation**
- [Understanding vGW Series Integration with vCloud Director on page 41](#)
 - [vGW Series Attributes for VMware on page 118](#)
 - [Understanding vGW Series Groups on page 111](#)
 - [Creating vGW Series Smart Groups for VMware on page 114](#)
 - *Understanding vGW Series*

CHAPTER 5

Policy-per-vNIC Feature

- [Understanding the vGW Series Policy per vNIC Feature on page 47](#)
- [Configuring the vGW Series Policy per vNIC Feature on page 50](#)
- [Configuring and Displaying vGW Policies for Individual vNICs on the Same VM on page 52](#)
- [Configuring Policy per vNIC to Secure Only Some of a VM's vNICs on page 55](#)
- [Understanding Policy per vNIC and Smart Groups for VMware Environments on page 55](#)

Understanding the vGW Series Policy per vNIC Feature

This topic covers the vGW Series Policy per vNIC feature that allows you to configure separate firewall policies for individual interfaces, or virtual NICs (vNICs), configured on the same VM.

Before you use Policy per vNIC, you should be familiar with how to secure VMs and manage firewall policies, and you should have an overall understanding of the configuration of VMs that include more than one vNIC.

This topic includes the following sections:

- [About Policy per vNIC on page 47](#)
- [Why Use Policy per vNIC on page 48](#)
- [vNICs With Individual Policies and Smart Groups on page 49](#)
- [Viewing vNICs With Individual Policies on page 49](#)
- [Naming Conventions for vNICs on page 50](#)

About Policy per vNIC

You use the Settings module vGW Application Settings > Install Settings > Policy Per vNIC pane to enable the Policy per vNIC feature. You can enable the Policy per vNIC feature or you can allow the default capability that secures all vNICs on a VM in the same way. If you enable Policy per vNIC, you can still configure a policy for a VM that has only one vNIC.

If you do not enable Policy per vNIC, you can not configure individual policies for any vNICs on a VM that has more than one vNIC. In that case, all of the VM's vNICs inherit the same policy.

If you enable the Policy per vNIC feature, you can enable an option that allows you to exempt one or more vNICs on the same VM from requiring a firewall policy, effectively bypassing firewall security. When you enable this option, you can secure some individual vNICs with their own policies and leave other vNICs on the same VM unsecured.

You enable or disable Policy per vNIC at the global level: its configuration applies to all VMs that you secure using the same vGW Security Design VM. You cannot disable Policy per vNIC when individual vNICs have active policies applied to them.

You create policies for vNICs using the Firewall Manage Policy page. [Figure 11 on page 48](#) shows the policy page for the vNIC1 that belongs to the IT-WWW-DEV VM.

Figure 11: Policy for Single vNIC



Why Use Policy per vNIC

Policy per vNIC satisfies many requirements that emerge in a virtualized environment. For example:

- If your environment includes more than one PortGroup/vSwitch, you might want to have different policies for each of the networks that their VMs connect to.
- Your environment might include a server that connects both to the front end for customer interaction and to the back end for storage and management. You might want to disable the firewall on the back end but enforce it on the front end. In this case, you could use **Enable opt-out of firewalling per vNIC** feature.
- Your environment might include a single VM that has multiple vNICs attached to it, some of which have IPv6 addresses bound to them and some of which have IPv4 addresses bound to them. You can use the Policy per vNIC feature to apply different policy rules to vNICs passing IPv4 traffic from those used for IPv6 traffic, even when the vNICs are attached to the same VM. You could configure specific addresses for source or destination terms or you could use the predefined terms **Any-IPv4** and **Any-IPv6**.

vNICs With Individual Polices and Smart Groups

VMs for which the Policy per vNIC feature is used can be included in Smart Groups. You can choose whether membership in a Smart Group applies to the entire VM, that is, all of its interfaces, or only the vNICs that the Smart Group logic applies to. For example, an interface (a single vNIC) might belong to a port group or be connected to a certain VLAN which could qualify its membership in a Smart Group. For details on the relationship between vNICs and Smart Groups when Policy per vNIC is configured, see [“Understanding Policy per vNIC and Smart Groups for VMware Environments”](#) on page 55.

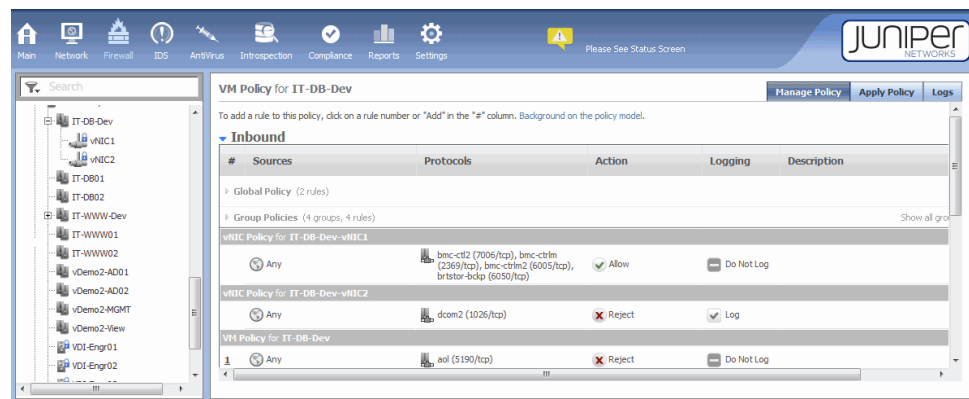
Viewing vNICs With Individual Policies

This section gives an overview of vNICs information as displayed by the vGW Security Design VM. See also [“Configuring and Displaying vGW Policies for Individual vNICs on the Same VM”](#) on page 52.

When the Policy per vNIC feature is enabled:

- vNICs are displayed under their VM in the VM Tree. The VM expands to show its individual vNICs. For example, as [Figure 12 on page 49](#) shows, IT-DB-Dev expands to show vNIC1 and vNIC2. Although this page shows the policy for the entire VM, you can select a vNIC and see only its policy.

Figure 12: VM with Multiple vNICs Shown in the VM Tree



- For operations that pertain to a VM, such as Introspection and Compliance, individual vNICs are not shown. They are treated in the same way as the VM that they belong to.

If a VM includes a vNIC that is not compliant, then the VM is considered noncompliant.

If you do not use the Policy per vNIC feature, the same policy is applied to all vNICs of a VM, and the VM is displayed as a single host in the VM Tree.



NOTE: When a vNIC with a policy is deleted, it no longer shows up in the list of vNICs with a policy. When you disable Policy per vNIC, the policies for all deleted vNICs are cleared. However these changes are not applied automatically. Consequently, if you create a vNIC again after having deleted it, the Apply Policy page for the VM might show that there are policy changes that have not been applied, but it would not state changes under Global, Group, and VM policies.

Naming Conventions for vNICs

vGW Series aligns with the convention for naming vNICs that is used by VMware in its vCenter:

- In VMware, naming of vNICs follows this convention: Network adapter 1, Network adapter 2, and so on. Numbering of vNICs begins with 1, not 0.
- In vGW Series, naming of vNICs follows this convention: VMx.nic1, VMx.nic2, and so on.

Related Documentation

- [Understanding vGW Series](#)
- [Configuring the vGW Series Policy per vNIC Feature on page 50](#)

Configuring the vGW Series Policy per vNIC Feature

This topic explains how to enable and configure the vGW Series Policy per vNIC feature that allows you to define separate policies for individual vNICs attached to the same virtual machine (VM).

Before you read this topic, read “[Understanding the vGW Series Policy per vNIC Feature](#)” on page 47.



NOTE: For VMs that have multiple vNICs, you can still use the default configuration that allows you to use the same policy for all vNICs on your VMs. You are not required to use Policy per vNIC.

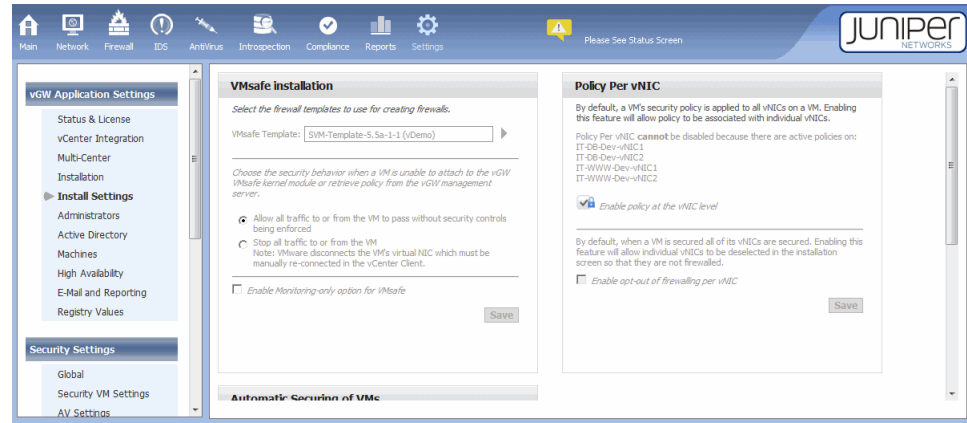
You can configure vNICs on the same VM to use:

- Separate policies for all vNICs on a VM.
- Separate policies on some vNICs on one VM while leaving other vNICs on the same VM unsecured.
- The same policy for all vNICs on a single VM (default).

You cannot disable Policy per vNIC when individual vNICs have active policies applied to them.

Figure 13 on page 51 shows the Install Settings page that you use to enable vGW Policy per vNIC and define its behavior.

Figure 13: Policy Per vNIC



To enable Policy per vNIC:

1. In the Settings module vGW Application Settings section, select **Install Settings**.
2. To enable the feature globally, in the Policy Per vNIC pane, select the **Enable policy at the vNIC level** check box.
3. Optionally, select the **Enable opt-out of firewalling per vNIC** check box if you want to secure some vNICs but not others on the same VM. See [“Configuring Policy per vNIC to Secure Only Some of a VM's vNICs” on page 55](#).

When new interfaces are added to a VM that includes vNICs that are not secured, the new vNICs are automatically secured. If you want them not to be secured, you must manually unsecure them. The following procedure explains how to remove security from a vNIC.

If you disconnect a vNIC from a port group, that is, un-selected it, the vNIC becomes unsecured. A warning message on the Installer dialog shows the state of the vNICs.



CAUTION: If you select “Enable opt-out of firewalling per vNIC” on the Policy Per vNIC pane, vNICs can not be secured individually if they belong to the same port group.

This procedure explains how to remove a security policy from a vNIC, that is, *unsecure* it. To unsecure a vNIC:

1. Select the vGW Security Design VM Settings module.
2. In the vGW Application Settings section, select **Installation**.
3. Before you unsecure the vNIC, delete any policies applied to it.
4. In the Secured Network pane, select the vNIC that you want to leave unsecured, and click the **Unsecure** arrow.

The vGW Security Design VM presents a message that asks you whether you want to unsecure the vNIC or the entire VM.

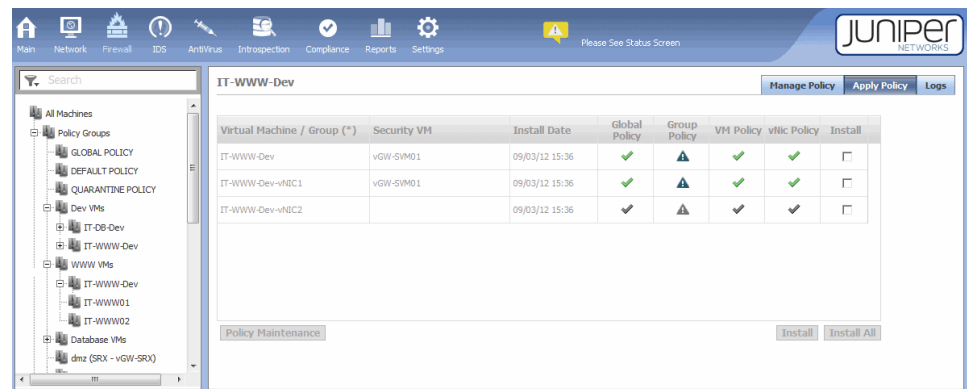
If you add a new vNIC to a VM that contains vNICs that are not secured, the new vNIC is automatically secured. If you want to unsecure it, you must do it manually as explained previously.

You use the Firewall module pages to create and apply policies for vNICs that belong to a VM with multiple vNICs and for which you use the Policy per vNIC feature.

Figure 14 on page 52 shows the Firewall module Apply Policy page for the IT-WWW-DEV VM with multiple vNICs. To apply the policies, you must select the **Install** check box and click **Install (Install All)**.

For details on how to define individual policies for vNICs, see “Configuring and Displaying vGW Policies for Individual vNICs on the Same VM” on page 52.

Figure 14: Applying Policy to Individual vNICs



Related Documentation

- [Understanding vGW Series](#)
- [Configuring Policy per vNIC to Secure Only Some of a VM's vNICs on page 55](#)

Configuring and Displaying vGW Policies for Individual vNICs on the Same VM

This topic covers how to configure policy rules for individual vNICs that belong to the same virtual machine (VM) when the Policy per vNIC feature is enabled. It also explains how vNICs are displayed in the VM Tree. You use the Firewall module of the vGW Security Design VM to configure and apply policies to vNICs.

When Policy per vNIC is enabled and multiple vNICs for the same VM have been configured they are presented in the VM Tree nested beneath the VM that they belong to.

The VM Tree displays the state of a vNIC in the following ways:

- The VM Tree displays the state of a vNIC in the following way:
 - A disabled vNIC is shown with an icon that indicates that traffic on the vNIC is not protected by the vGW Security VM firewall.

- If a VM contains vNICs with individual firewall policies and the VM belongs to a group, the vNICs that are members of the group are shown as active. The vNICs that do not belong to the group are shown, but they are grayed out indicating that they are not part of the group.



NOTE: vNIC numbers can change when one vNIC is deleted. For example, if a VM contains vNIC1 and vNIC2 and you remove vNIC1, then vNIC2 becomes vNIC1. If you have manually created policies for both vNIC1 and vNIC2, the enforced policy is also changed so that the correct policy for the vNIC remains with it.

- vNICs are displayed in the VM Tree:
 - If more than one vNIC is configured for a VM.
 - When there remains one vNIC configured for a VM and a policy is applied to it.
In this case, originally there were multiple vNICs configured for the VM, each with its own policy, and all except one of them was deleted. It is still possible for you to edit or delete the policy on the remaining vNIC.

vNIC policies are shown above the policy for the VM that they belong to, in the order in which they were defined.

- vNIC policies are enforced after the policy for the VM that they belong to.
- When you select a VM in the VM Tree, policies for the vNICs that belong to it are shown as read-only.
- When you select a vNIC in the VM Tree, the policy for that vNIC is shown, and you can edit it. All other policies are shown as read-only. Policies for other vNICs are not displayed.
- From the perspective of the rule base, vNIC policies behave in the same way as other policy types:
 - If the vNIC is selected in the VM Tree, the policy for it can be edited. If the VM is selected, the vNIC policies are greyed out indicating that they can not be edited.
 - For unsecured vNICs, the vNIC header is shown. Instead of rule information, the following message is displayed: "This interface is configured to bypass firewall enforcement".

When Policy per vNIC is enabled, the Apply Policy table reflects the vNIC configuration in the following way:

- vNICs are displayed as rows in the Apply Policy table. When Policy per vNIC is disabled or a VM does not contain multiple vNICs, the table displays information for the VM as usual. See *Understanding the vGW Series Firewall Module* for details on the Apply Policy table.
- When you select the VM in the VM Tree, the policy for it is displayed. However, there is a table entry for each vNIC, but it reads "(no rules)".

- Each vNIC has its own policy. If all vNICs except one are removed from the VM, the remaining vNIC is displayed in the table. Its policy can be edited or deleted.



NOTE: You can not disable the Policy per vNIC feature if there are policies configured for any vNIC or groups containing the vNIC. You must first delete the policies.

You use the Firewall module Manage Policy tab to add rules for individual vNICs in the same way that you configure other policy rules.

This procedure explains how to define policies for the following example. For additional details on how firewall policy rules are configured, see *Understanding the vGW Series Firewall Module*.

This example assumes that the Policy per vNIC feature is enabled. For details on how to enable Policy per vNIC, see [“Configuring the vGW Series Policy per vNIC Feature” on page 50](#). The example assumes that the administrator wants to configure separate policies for each of the following three vNICs on a VM called MIS-Fileserver that is used as a file server:

- vNIC1 (MIS-Fileserver-vNIC1) is dedicated to network connections, and it requires a policy whose protocol specification allows https and ssh traffic.
- vNIC2 (MIS-Fileserver-vNIC2) whose policy allows the iSCSI protocol to use to link data storage facilities.
- vNIC3 (MIS-Fileserver-vNIC3) that is used for management that allows SNMP protocol traffic.

To configure policies for these vNICs:

1. In the vGW Security Design VM, select the Firewall module.
2. In the VM Tree, locate the MIS-Fileserver VM, and expand it to display the vNICs.
3. Select vNIC1.

When you select the vNIC, the policy page for it is displayed. The policy is called vNIC Policy for MIS-Fileserver-vNIC1.

4. Beneath the Global Policy line is a line labeled “vNIC Policy for MIS-Fileserver-vNIC1” that allows space for you to enter a policy rule for the vNIC.

Click **Add**.

5. In the Sources column for the rule, leave **Any**.
6. In the Protocols column for the rule, click **Any** to display a list of protocols.
 - a. In the Filter box, enter **https**. The list is scrolled to https (443/tcp). Select it and click the right-facing **Arrow** to move it to the Selected Protocols box.
 - b. In the Filter box, enter **ssh**. The list is scrolled to ssh(22/tcp). Select it and click the right-facing **Arrow** to move it to the Selected Protocols box.

Click **Save**.

When Policy per vNIC is enabled, the Apply Policy table contains an additional column to indicate policy state for the vNIC.

**Related
Documentation**

- [Understanding vGW Series](#)
- [Understanding Policy per vNIC and Smart Groups for VMware Environments on page 55](#)

Configuring Policy per vNIC to Secure Only Some of a VM's vNICs

The Policy per vNIC feature includes an option that allows you to secure some of your vNICs and leave others unsecured. To use this option, you must enable Policy per vNIC. You use the Policy per vNIC pane on the Install Settings page to enable Policy per vNIC and to select the Enable opt-out of firewalling per vNIC option.

If you select the Enable opt-out of firewalling per vNIC option, the unit of configuration is the VM and port group. That is, vNICs cannot be secured individually if they belong to the same port group. This behavior protects against your having a secured and an unsecured connection to the same port group.



NOTE: When new interfaces are added to a VM that includes vNICs that are not secured, the new vNICs are automatically secured. If you want them not to be secured, you must manually unsecure them.

**Related
Documentation**

- [Understanding vGW Series](#)
- [Configuring and Displaying vGW Policies for Individual vNICs on the Same VM on page 52](#)

Understanding Policy per vNIC and Smart Groups for VMware Environments

You use the vGW Security Design VM Settings module vGW Application Settings > Install Settings > Policy Per vNIC pane to enable the Policy per vNIC feature. When it is enabled, you can add individual vNICs to a Smart Group. When you configure a Smart Group, you can specify whether requirements for membership in the group apply to an entire VM, that is, all of its interfaces, or only to the vNICs that the logic pertains. For example, Smart Group criteria might specify that the vNIC must belong to a port group or that it must be attached to a VLAN to gain membership in the group.

The ability to configure Smart Groups for vNICs is available only when Policy per vNIC is enabled. You can configure this information when **Advanced Attributes** is selected.

After you configure the group, you can test it. When you click **Test**, the results show the vNIC extensions, not just the VM name.

You can use the following Smart Group attributes to configure groups to include vNICs. These attributes do not pertain to the VM as a whole.

Table 3: Smart Group Attributes for vNICs When Policy per vNIC Is Enabled

Smart Group Attribute Definition	Data Type	Comment
vf.firewall	String	Is this VM a vGW Security VM?
vf.group	Multi String	Comma-separated string of all vGW groups to which a VM belongs.
vf.has_installed_group_policy	Boolean	Does the VM have a non-default group policy installed?
vf.has_installed_policy	Boolean	Does the VM have an installed security policy?
vf.monitored	Boolean	Is the VM currently being monitored by the vGW Security Design VM?
vf.secured	Boolean	Is a VM currently secured by the vGW Security Design VM?
vf.secured_active	Boolean	Is the VM actively protected by vGW?
vi.host.vmkernel.isolated.vlan	Boolean Value	Is the vmkernel management network on this hypervisor on an isolated VLAN?
vi.host.vmkernel.isolated.vswitch	Boolean Value	Is the vmkernel management network on this hypervisor on an isolated vSwitch?
vi.ipv4	IPv4 (multi value)	The IP addresses as known on a VM.
vi.ipv6	IPv6 (multi value)	<p>The IP addresses as known on a VM. They can be coded as single addresses or an address range.</p> <p>Example Addresses:</p> <ul style="list-style-type: none"> • 2001:0db8:5a3:0000:0000:0000:0000:0370:7334 • fe80::202:b3ff:fe1e:8329
vi.pg_security.forgedtransmits	Boolean Value	Is VM connected to a port group which allows forged MAC addresses (MACs other than defined in the VMX)?
vi.pg_security.macchanges	Boolean Value	Is VM connected to a port group which allows reception of unknown MAC addresses (MACs other than defined in the VMX)?
vi.pg_security.promiscuous	Boolean Value	Is VM connected to a promiscuous port group?

Table 3: Smart Group Attributes for vNICs When Policy per vNIC Is Enabled (*continued*)

Smart Group Attribute Definition	Data Type	Comment
vi.portgroup	String Value	Port groups on the virtual switch this VM is actively connected to. Port Groups for disconnected vNICs will not be included. (For a running/suspended VMs this will be the port groups actually connected. For a stopped VM, this value is the port groups that are connected at power-on.)
vi.portgroup.all	String Value	Port groups on the virtual switch this VM configured to be connected to, this list includes port groups even if the vNIC is disconnected. (For a running/suspended VMs this will be the port groups actually connected. For a stopped VM, this value is the port groups that are connected at power-on.)
vi.pvlan	Numeric Value	Private VLAN values for connected port groups.
vi.pvlan.all	Numeric Value	List of all Private VLANs in use by this VM, includes vNICs in both connected and disconnected states.
vi.vlan	Multi-value integer	VLANs of connected port groups.
vi.vlan.all	Multi-value integer	VLANs of all interfaces.
vi.vmsafe_configured	Boolean	Is VMsafe firewall security enabled for this VM?
vi.vmsafe_dvfilter	Multi String	The dvfilters protecting this VM.
vi.vmsafe_initfailmode	Enumeration	If VMsafe is unable to initialize, what is the network connectivity choice for this VM?
vi.vnic.count	Numeric Value	Number of connected vnics.
vi.vswitch	Multi String	vSwitch VM is connected to.

You use the attributes shown in [Table 3 on page 56](#) to define a Smart Group. The Smart Group editor has two modes: basic and advanced. Basic mode lets you select one to many attributes and assign an All or Any constraint. You simply add rules by clicking the + sign. Advanced mode allows you to configure the Smart Group for vNICs.

1. In the Security Settings section of the vGW Security Design VM Settings module, select the **Groups** subsection.
2. Click **Add Smart Group** on the displayed page.

3. Click **Advanced** at the top of the page to display vNIC group options.
4. In the Add Group definition pane, enter a name for the Smart Group. For this example, enter **Apache Web Servers**.
5. Click **Enable vNIC membership** to specify that group membership pertains to vNICs, and not the VM.
6. Select the **All** option button in the Matches section.
7. Click the down arrow to display a list of attributes. Select the attribute **vi.name**, select **Contains**, and enter **www**.
8. Click the **+** mark at the end of the row to display another row.
9. Select the attribute **vf.application**, select **Contains**, and enter **www**.
10. Under Group Attributes, select **Policy Group** allow a policy to be associated with this group.
11. Select **Medium** as the Priority level, and assign it a precedence of **2** in the Precedence within Level.
12. Select Manual.

This allows you to use the Settings module and apply a policy to the group using the Firewall Apply Policy tab.

1. Specify a name for the group and configure its attributes.
2. Click **Enable vNIC membership** to specify that group membership pertains to vNICs, and not the VM.
3. Click **Test** to view the results of your configuration.

The test results show the VM name with the vNIC extension that the Smart Group logic applies to.

When you view a Smart Group in the VM Tree and display the VM with its nested vNICs, vNICs that belong to the group—that satisfy the group's logic criteria—are displayed as usual. vNICs that do not belong to the group are greyed out.

Whether a vNIC is secured or not is indicated as usual for all of the VM's vNICs.

**Related
Documentation**

- *Understanding vGW Series*
- [Configuring and Displaying vGW Policies for Individual vNICs on the Same VM on page 52](#)

CHAPTER 6

Split-Center and Multi-Center Features

- [Understanding the vGW Series Split-Center Feature on page 59](#)
- [Understanding the Multi-Center Feature on page 63](#)
- [Configuring vGW Series Multi-Center on page 66](#)
- [Understanding vGW Series Multi-Center Synchronized Objects on page 69](#)
- [Configuring Scaling Using the Multi-Center and Split-Center Features on page 70](#)

Understanding the vGW Series Split-Center Feature

This topic covers the vGW Series Split-Center feature that allows you to segment resources contained in a single VMware vCenter into multiple domains, or scopes, independently managed by different vGW Security Design VMs. The Split-Center feature allows for improved resource isolation for cloud services and multi-tenancy. It supports unlimited scalability as the VMware vCenter capacity increases and your deployment takes advantage of it. You can deploy as many vGW Security Design VMs as are needed as you scale your environment.

Together the individual vGW Security Design VMs associated with a vCenter can collectively secure all its ESX/ESXi hosts and VMs, but each individual vGW Security Design VM manages only a specific set of resources, determined according to how you configure the management scope for that vGW Security Design VM. One vGW Security Design VM does not have visibility into another vGW Security Design VM or the parts of the virtualized environment that another vGW Security Design VM secures. After you configure its management domain, to a single vGW Security Design VM it is as if all objects outside its scope do not exist.

The Split-Center feature allows you to configure management domains that consist of:

- entire vCenter

You can select the entire vCenter as the management scope. Effectively you are not using the Split-Center feature in this case.

- Multiple data centers

Ensure that each data center is assigned to only one vGW Security Design VM. Otherwise, unexpected consequences can occur.

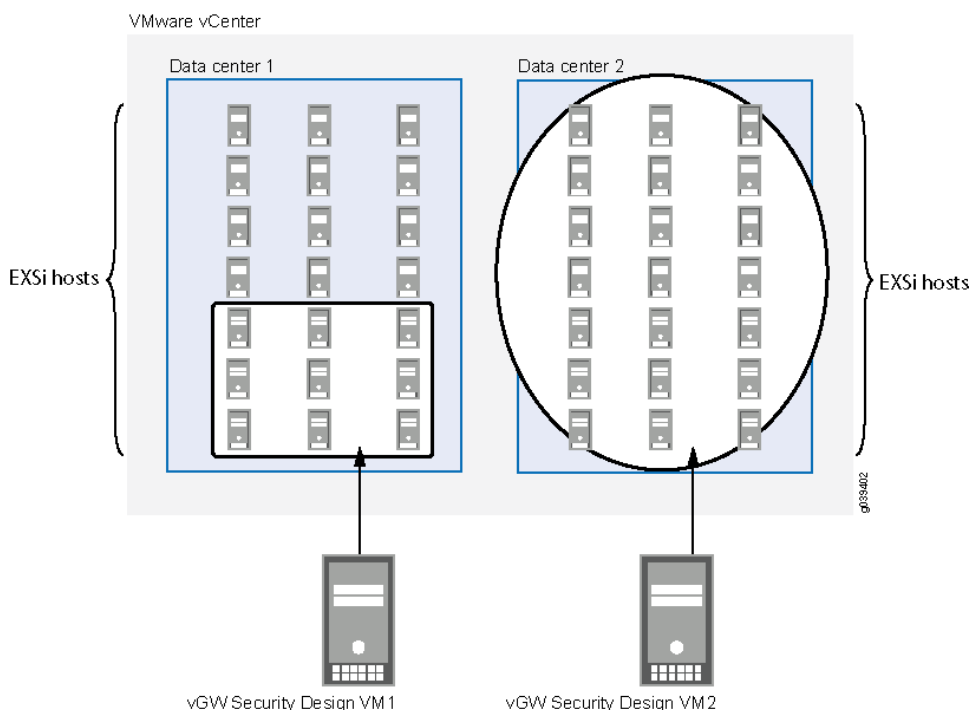
- One or more clusters of hosts within a data center

In some environments, organizations use clusters of host to segment their virtual infrastructure rather than data centers. To support these environments, you can configure the Split-Center feature along lines of host cluster management domains.



NOTE: All of the host clusters that you select to belong to a management domain (scope) must be in the *same* data center. You can not include host clusters from two or more different data centers in the scope.

The following figure shows a vCenter with two data centers. Nine of the hosts in Data center 1 comprise a cluster that is configured as a domain to be secured and managed by vGW Security Design VM1. The remaining hosts in data center 1 are not secured by vGW Series. All of the hosts in Data center 2 are configured as a single domain to be managed and secured by vGW Security Design VM2.



As the administrator who oversees your deployment, most likely you determine the management domains for your virtualized environment. Afterward, you can convey to administrators of the individual vGW Security Design VMs for the vCenter which objects to include in their management scopes.

Administrators of various vGW Security Design VMs establish their management domains when they run the vGW Installation Wizard to initially set up their vGW Security Design VM. See *Setting Up vGW Series* for details on initially setting the management domain.

The following figure shows how to configure the management scope, or domain during installation.

Figure 15: Configuring the Management Scope During Installation to Include Clusters

If you change the management domain deployment design later, administrators can reconfigure the Split-Center domains that their vGW Security Design VMs manage using the Settings module vGW Application Settings > vCenter Integration > vCenter Settings pane called *Select a scope for your Security Design vGW*.

For both the initial management domain configuration during product installation and when you change the configuration, the same vCenter Settings pane is used, but it is approached differently.

Depending on how you define your management domain, you configure a vGW Security Design VM for Split-Center in either of the following ways:

- **Datacenter**—A subset of data centers in the vCenter.

In this case, the vGW Security Design VM is able to access and manage only the VMs and other entities in the selected data centers.

To use this scope:

1. Select **Datacenters**.

vGW Series displays all of the vCenter's data centers.



NOTE: To update the list of data centers at any time to show changes—datacenters that might have been added or removed—click **Refresh**.

2. Select the data centers for your vGW Security Design VM to manage.

Ensure that each data center is assigned to only one vGW Security Design VM. Otherwise, unexpected consequences can occur.

3. Click **Save**.

- **Clusters**—A subset of host clusters in a data center. In this case, the vGW Security Design VM is able to access only the VMs and other entities on the selected host clusters.

To use the Clusters scope:

1. Click **Clusters** in the *Select a scope for your Security Design vGW* area.
vGW Series displays a list of available data centers in response.
2. Select a data center from the displayed list whose host clusters you want the vGW Security Design VM to manage.
 - a. Click the arrow at the end of the box beside **Datacenter:** to display a list of data centers for the vCenter.
 - b. Click the data center whose cluster(s)/host(s) you want your vGW Security Design VM to manage.
vGW Series displays a list of cluster(s)/host(s) for the data center that you selected.
3. Select the check box before the names of the cluster(s)/host(s) that you want to include in your management domain. All host clusters that you select must belong to the same data center.
4. Click **Save**.



NOTE: Ensure that each host cluster is assigned to only one vGW Security Design VM. Otherwise, unexpected consequences can occur.

You can change the cluster selection at any time. However, when you change the cluster scope, either of the following conditions can occur:

- Some vGW Security VMs could become unmanaged—This can occur when you remove a cluster from the list of selected clusters. Any vGW Security VM installed on an ESX/ESXi host that belongs to the removed cluster will no longer be accessible, and therefore it is no longer managed by the vGW Security VM.
- Some unmanaged vGW Security VMs could become accessible—If ESX/ESXi hosts that belong to a cluster that you add to your vGW Security Design VM management domain had a vGW Security VM installed on them by a different vGW Security Design VM, you could gain access to the vGW Security VMs. It is possible and important to gain access to an unmanaged vGW Security VM when you add its host cluster to your vGW Security VMs management domain for the following reason.

When a vGW Security VM becomes inaccessible because of cluster or datacenter selection changes its original vGW Security Design VM, its operational state might be compromised unless it is imported into another vGW Security Design vGW. This is because the vGW Security VM continues to try to communicate with its original vGW Security Design VM, which no longer recognizes it as a managed.

To view a list of unmanaged SVMs and render them manageable again:

1. Display the Settings module > Security VM Settings page.

The unmanaged vGW Security VMs are identified by a gray triangle status indicator.

2. To make a vGW Security VM manageable again, click its row to select it.
3. Click **Import**.

- Clusters

To configure a domain that contains clusters:

1. Select **Clusters** in the *Select a scope for your Security Design vGW* area.
2. Select a data center.
 - a. Click the arrow at the end of the box beside **Datacenter:** to display a list of data centers for the vCenter.
 - b. Click the data center whose cluster(s)/host(s) you want your vGW Security Design VM to manage.

vGW Series displays a list of cluster(s)/host(s) for the data center that you selected.

3. Check the boxes before the names of the cluster(s)/host(s) that you want to include in your management domain.

You can define the management scope initially using the vGW Installation Wizard when you set up your vGW Security VM. You can use the same page later to change the configuration by selecting the Settings module vGW Application Settings > vCenter Integration > vCenter Settings page *Select a scope for your Security Design vGW* area.



NOTE: When you configure the management domain scope, you can select the entire vCenter. Effectively, Split-Center is not used in this scenario because a single vGW Security Design VM is responsible for all data centers in the vCenter.

Related Documentation

- [Understanding vGW Series](#)
- [Configuring Scaling Using the Multi-Center and Split-Center Features on page 70](#)
- [Configuring vGW Series Multi-Center on page 66](#)
- [Understanding the vGW Security Design VM](#)

Understanding the Multi-Center Feature

This topic covers the vGW Series Multi-Center feature that synchronizes policy across vGW Security Design VM management centers to enable large scale virtualization. The

Multi-Center feature is useful for large-scale virtualized environment deployments spread across many vCenters.

This section includes the following sections:

- [The Multi-Center Feature on page 64](#)
- [Deploying vGW Series in an Environment With a Mix of Delegate and Stand-alone vGW Security Design VMs in Various vCenters on page 65](#)

The Multi-Center Feature

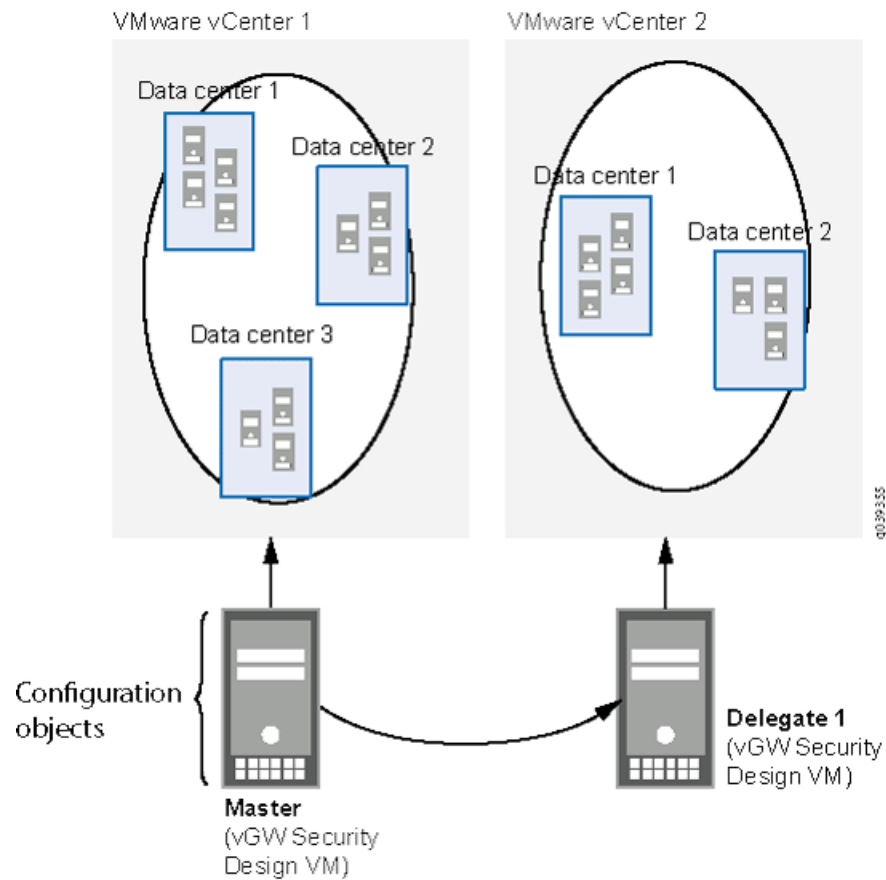
For various reasons—such as geographic separation of data centers, scaling requirements, and use of different administrative domains—some companies who deploy the vGW Series must use more than one VMware vCenter to manage their environments. These companies want to use the same or similar vGW Security Design VM configuration for all of their data centers, as if they were rolling out a single deployment. Manually configuring separate vGW Security Design VMs at various locations with the same information consumes time, and it is cumbersome and error prone.

To accommodate companies with these requirements and companies that want to scale their environments for other reasons, the vGW Series includes a feature called Multi-Center. The Multi-Center feature allows you to designate a single vGW Security Design VM connected to a vCenter at one location as the master.

Following the database replication model, configuration is done at master vGW Security Design VM. It can be synchronized all or in part to one or more delegate vGW Security Design VM centers, each of which is connected to an individual vCenter. Configuration of global objects at the master vGW Security Design VM is propagated to the delegate vGW Security Design VMs centers automatically, based on objects selected when the administrator of the master vGW Security Design VM creates a Multi-Center definition for the delegate center.

[Figure 16 on page 65](#) shows a master center and a delegate center. Objects at the master center are synchronized to the delegate center.

Figure 16: vGW Series Multi-Center



Deploying vGW Series in an Environment With a Mix of Delegate and Stand-alone vGW Security Design VMs in Various vCenters

The vGW Security Design VM Multi-Center feature can be in whatever configuration your environment requires. You might design your virtualized environment to include some vGW Security Design VMs that belong to a configuration that uses the Multi-Center feature and some that do not. You might want one vGW Security Design VM to manage resources at a specific vCenter and let it have an entirely unique configuration. You might want others at different vCenters to use largely the same configuration.

For example, an organization's virtualized environment might include six data centers of various sizes, each of which is connected to an individual vCenter. The administrator uses the same overall configuration for five of the data centers but not for the sixth one. The Multi-Center feature suits this environment well also in that it can secure the five data centers in the same way, but the administrator of the vCenter environment with different security requirements could define his own policies and other security protection independently.

Related Documentation

- [Configuring vGW Series Multi-Center on page 66](#)

Configuring vGW Series Multi-Center

This topic explains how to configure the Multi-Center feature which allows you to synchronize the configuration at one vGW Security Design VM across multiple vGW Security Design VMs connected to different VMware vCenters. The Multi-Center feature allows you to streamline configuration across multiple vGW Security Design VMs and coordinate various aspects of security as you scale. It relies on the configuration at one vGW Security Design VM, referred to as the master center, which is synchronized in part or whole to other vGW Security VMs, referred to as delegate centers.



NOTE: You can also use Multi-Center with the Split-Center feature to synchronize the configuration across multiple vGW Security Design VMs that manage resources in the same vCenter.

Before you read this topic, read [“Understanding the Multi-Center Feature” on page 63](#).

This topic contains the following sections:

- [vGW Security Design VM Master Center on page 66](#)
- [vGW Security Design VM Delegate Centers on page 66](#)
- [Configuring Multi-Center on page 67](#)

vGW Security Design VM Master Center

As administrator of the master center, you configure the object synchronization for all delegate centers—at the master vGW Security Design VM. After you configure the vGW Security Design VM that you will use as the master center, you can define delegate center configurations for individual delegate centers.

Although you configure Multi-Center for all delegate centers, each delegate center has its own independent configuration, and they can differ. When you add a delegate center configuration, you designate the objects that are synchronized to it.



NOTE: The master vGW Security Design VM and the delegates must be able to communicate using addresses from the same IP protocol family. Communication problems should not exist if this is the case. Too, if either of them is configured for dual stack, problems should not exist. If both are configured with a single IP from different protocol families, problems could ensue. To solve this problem, you could change the IP address used for one of them.

vGW Security Design VM Delegate Centers

Administrators of the master and delegate centers cooperate in implementing Multi-Center. They determine the objects to synchronize to the delegate center from the master center. Each delegate center has its own configuration at the master center.

Configuration objects, such as policies, configured at the master center that are synchronized to delegate centers are viewed as global objects from the perspective of the delegate center. Some delegate centers might not synchronize a certain object, but rather retain their own local configuration for that object. For information about configuration objects and how they are synchronized, see [“Understanding vGW Series Multi-Center Synchronized Objects”](#) on page 69.

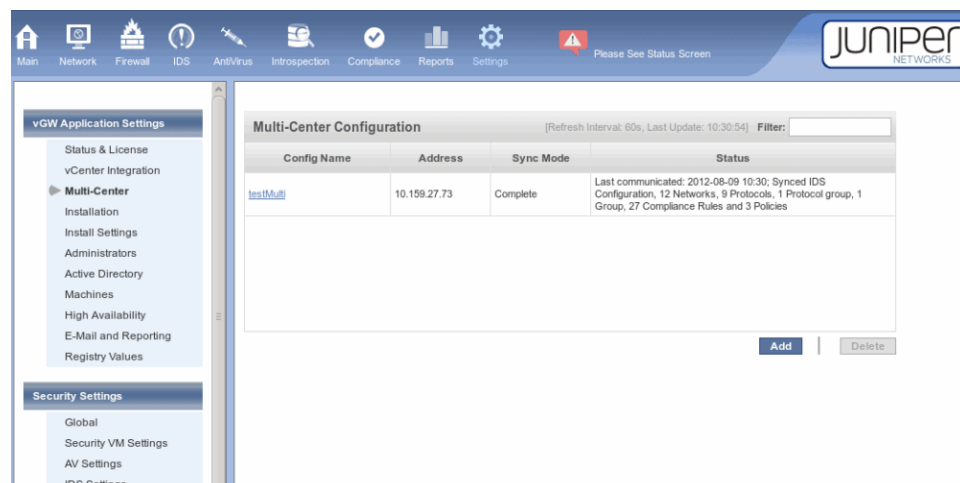
A vGW Security Design VM delegate center is created for a vCenter no differently from how it would be if it were independent. You import the OVA into the vCenter to be secured. For information on how to integrate vGW Series with vCenter, see *Using the OVA Bundled Method to Integrate vGW Series with the VMware Infrastructure*. After the installation is complete, you can begin to engage the vGW Security VM in the Multi-Center configuration.

Configuring Multi-Center

To configure Multi-Center, use the Settings module vGW Application Settings > Multi-Center page on the master center. To add a delegate center to the Multi-Center configuration:

1. At the bottom Multi-Center Configuration pane, click **Add**. See [Figure 17 on page 67](#).

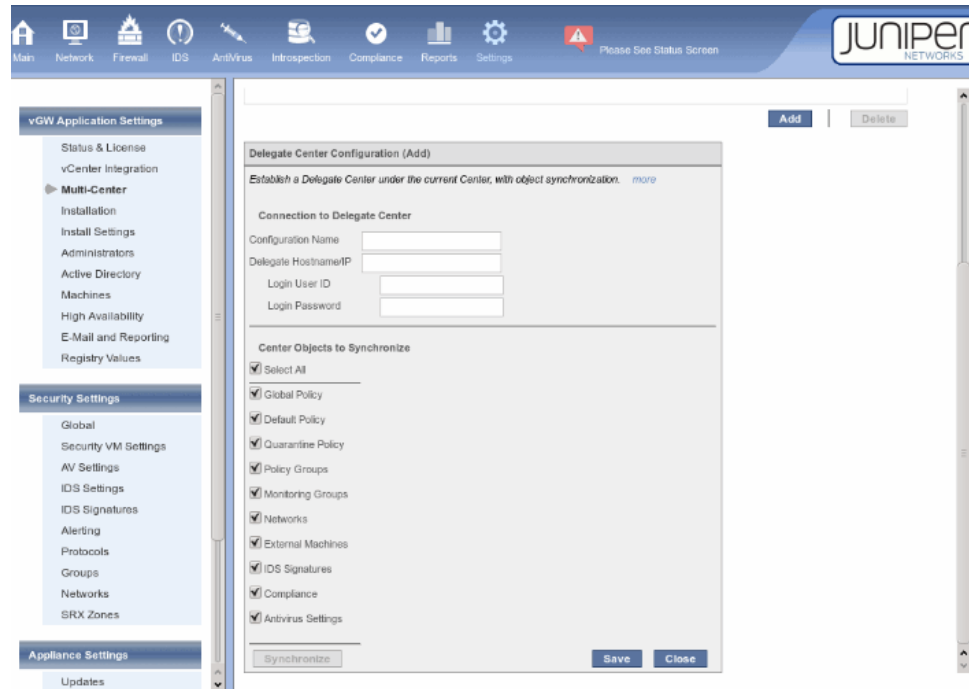
Figure 17: Multi-Center Configuration Page at Master vGW Security Design VM



The Delegate Center Configuration (Add) pane is displayed on the master vGW Security Design VM.

2. In the **Configuration Name** field, specify a name for the configuration that represents the delegate center. Note that the name field is used only for reference, and it can be anything. It does not need to match the name of the delegate vGW Security Design VM. See [Figure 18 on page 68](#).

Figure 18: Delegate Center Configuration on the Master vGW Security Design VM



3. In the **Delegate Hostname/IP** field, enter the name or the IP address of the delegate center.

Enter a valid hostname, IPv4 address, or IPv6 address.

4. In the **Login User ID** and **Login Password** fields, enter the delegate center's authentication information.
5. In the **Center Objects to Synchronize** pane, select the objects to synchronize.
 - Check **Select All** if you want the state of all of the objects in the list to be synchronized from the master vGW Security Design VM to the delegate center that you are defining.
 - If you want only some of the objects to be synchronized from the master vGW Security Design VM to the delegate center, select the check box before each object to synchronize.
 - Global Policy—Synchronizes the global policy and all objects it depends on. Among other objects, configurations for the source and destination of the rules in the policy and the protocols are copied.
 - Default Policy—Synchronizes the default policy and all objects it depends on. Among other objects, configurations for the source and destination of the rules in the policy and the protocols are copied.
 - Quarantine Policy—Synchronizes the quarantine policy and all objects it depends on. Among other objects, configurations for the source and destination of the rules in the policy and the protocols are copied.

- Policy Groups—Synchronizes all the policy groups and policies associated with them, and all objects that they depend on. Among other configurations, the sources and destinations of the rules in the policies, the protocols, the networks and the machines in the groups are copied.
- Monitoring Groups—Synchronizes all the monitoring groups and the policies associated with them, and all objects that they depend on. Among other configurations, the sources and destinations of the rules in the policies, the protocols, the networks and the machines in the groups are copied.
- Networks—Synchronizes all networks.
- External Machines—Synchronizes all external machines.
- IDS Signatures—Synchronizes IDS Signatures and Settings.
- Compliance - Synchronizes compliance rules and all objects that they depend on, such as groups.
- Antivirus Settings—Synchronizes all AntiVirus scan configurations, and all objects that they depend on, such as groups.

**Related
Documentation**

- [Understanding vGW Series](#)
- [Understanding vGW Series Multi-Center Synchronized Objects on page 69](#)

Understanding vGW Series Multi-Center Synchronized Objects

This topic explains how protocols and compliance rules objects are synchronized from the master vGW Security Design VM to the delegate vGW Security Design VM center. The Settings pane of the delegate center shows status and other information about objects that are synchronized to it.

From the perspective of a delegate center, the synchronized objects are viewed as read-only global objects, and they cannot be modified.

This topic includes the following sections:

- [Object Synchronization on page 69](#)
- [Object Naming on page 70](#)
- [Creation of Objects Local to the Delegate vGW Security VM on page 70](#)

Object Synchronization

It can occur that a newly synchronized global object is identical in name and content to a local object on the delegate center. In this case, for global objects that contain default values such as protocols and compliance rules, the local object is converted to a global one. The global version of the local object on the delegate center vGW Security Design VM is marked as converted. All references to the local object are preserved, but now they pertain to the global object. Because the converted object is now a global object, it is accessible as a read-only object on the delegate center vGW Security Design VM. That is, the administrator of the delegate center vGW Security Design VM cannot modify it.

When an object is no longer mirrored, it is deleted from the delegate center unless it is used by local objects. That is, if it was converted from a local object such as a protocol, it is converted back to the local object at that time.

Object Naming

To avoid naming issues and Smart Group logic problems, when the same name for a global object and a local object exists in the same context, the global object takes precedence and the name is used for it. vGW Series marks the object as global, as viewed from the delegate center. The object with the conflicting name is renamed with the word local appended to it.

The administrator of the master vGW Security Design VM can remove an object from selection for a delegate center. In this case, the object is no longer a global one on the delegate center. If a local counterpart exists, it is now reinstated and the delegate center administrator can edit it.

Creation of Objects Local to the Delegate vGW Security VM

Administrators of delegate vGW Security Design VMs centers are still able to configure local objects for their own systems. These local objects remain local, and they have no affect on the master vGW Security Design VM configuration, with some exceptions. For example, the priority of local policy groups is always lower than global ones.

Related Documentation

- [Understanding the Multi-Center Feature on page 63](#)
- [Understanding vGW Series](#)
- [Understanding the vGW Security Design VM](#)

Configuring Scaling Using the Multi-Center and Split-Center Features

This topic explains how to use the vGW Series Split-Center and Multi-Center features together to secure your virtualized environment as you scale.

These features are typically used together to:

- Allow for partitioned management of resources among multiple vGW Security Design VMs at an individual vCenter.

The Split-Center feature allows you to segment responsibility for portions of your resources at an individual vCenter among multiple vGW Security Design VMs. It is as if each vGW Security Design VM were connected to an individual vCenter.

For background on the Split-Center feature, read [“Understanding the vGW Series Split-Center Feature” on page 59](#).



CAUTION: When you configure the Split-Center feature, ensure that each data center is assigned to only one vGW Security Design VM. Otherwise, unexpected consequences can occur.

- Deploy largely the same configuration to all vGW Security Design VM delegate centers, including those that share responsibility for a single vCenter.

The Multi-Center feature facilitates configuration management as you scale your environment. You can use it to create configurations that are largely the same for vGW Security Design VMs at different vCenters and for vGW Security Design VMs sharing security management responsibility for resources at the same vCenter. You can effectively deploy the same configuration to them automatically with real-time updates.

For background on the Multi-Center feature, see [“Understanding the Multi-Center Feature” on page 63](#).

This topic contains the following sections:

- [vGW Series Split-Center Multi-Center Configuration Requirements on page 71](#)
- [About the Example on page 72](#)
- [Configuring Split-Center and Multi-Center for vGW Security Design VMs on page 74](#)

vGW Series Split-Center Multi-Center Configuration Requirements

This example addresses a customer environment with a virtualized infrastructure that includes data centers at three individual VMware vCenters:

- The first vCenter, vCenter1, includes five customer data centers. vCenter1 is located in Dallas, Texas. One data center is considerably larger than the others.

The customer uses the Split-Center feature to partition management of the vCenter1 data centers among two vGW Security Design VMs in the following way:

- vGW Security Design VM-1 manages the large data center, vCenter1-data-center-1.
- vGW Security Design VM-2 manages the other four data centers:
 - vCenter1-data-center-2.
 - vCenter1-data-center-3.
 - vCenter1-data-center-4.
 - vCenter1-data-center-5.
- The second vCenter, vCenter2, includes two customer data centers. vCenter2 is located in Minneapolis, Minnesota. vGW Security Design VM-3 manages both:
 - vCenter2-data-center-1.
 - vCenter2-data-center-2.
- The third vCenter, vCenter3, includes two data centers. vCenter3 is located in Raleigh, North Carolina. vGW Security Design VM-4 manages both:
 - vCenter3-data-center-1.
 - vCenter3-data-center-2.

About the Example

This customer's virtualized environment spans three vCenters at various locations. The customer plans to use the Split-Center feature to divide security management responsibility for resources at one of the vCenters among two vGW Security Design VMs.

The customer plans to deploy largely the same configuration for all vGW Security Design VMs. Because manually creating separate configurations with the same parameters is time consuming and error prone, the customer decides to use the Multi-Center feature to solve this problem.

The Multi-Center feature allows the customer to use a single vGW Security Design VM as the master center. Its configuration is copied to all slave, or delegate, vGW Security Design VMs.

For this example, vGW Security Design VM-3 serves as the primary center. The administrator of vGW Security Design VM-3 configures the Multi-Center feature for all delegate centers.

Using the Settings module Application Settings > Multi-Center, the administrator defines an entry for each delegate vGW Security Design VM center. For this example, delegate centers include:

- vGW Security Design VM-1

The configuration specifies that all objects are to be copied.

- vGW Security Design VM-2

The configuration specifies that all objects are to be copied.

- vGW Security Design VM-4

The configuration specifies that all objects excluding monitoring groups and IDS are to be copied.

You use the Delegate Center Configuration (Add) pane of the Settings module Multi-Center feature to create an entry for a delegate vGW Security Design VM center. See [Figure 19 on page 73](#).

Figure 19: Delegate Center Configuration on the Master vGW Security Design VM

The screenshot shows the Juniper Networks vGW Security Design VM interface. The left sidebar contains navigation menus for vGW Application Settings, Security Settings, and Appliance Settings. The main content area displays the 'Delegate Center Configuration (Add)' dialog. This dialog is used to establish a delegate center under the current center, with object synchronization. It includes fields for Configuration Name, Delegate Hostname/IP, Login User ID, and Login Password. Below these fields is a section titled 'Center Objects to Synchronize' with a list of objects and checkboxes to select them. The objects listed are: Select All, Global Policy, Default Policy, Quarantine Policy, Policy Groups, Monitoring Groups, Networks, External Machines, IDS Signatures, Compliance, and Antivirus Settings. At the bottom of the dialog are buttons for Synchronize, Save, and Close. The top of the interface shows a navigation bar with icons for Main, Network, Firewall, IDS, Antivirus, Inspection, Compliance, Reports, and Settings, along with a status message 'Please See Status Screen'.

To do so, you provide the following information:

- In the **Configuration Name** field, specify a name for the configuration that represents the delegate center.



NOTE: Note that the name field is used only for reference, and it can be anything. It does not need to match the name of the delegate vGW Security Design VM.

- In the **Delegate Hostname/IP** field, enter the name or the IP address of the delegate center. This allows the master vGW Security Design VM and the delegate center vGW Security Design VM to communicate.
- In the **Login User ID** and **Login Password** fields, enter the delegate center's authentication information.
- In the **Center Objects to Synchronize** pane, select the objects to synchronize.
 - Check **Select All** if you want the state of all of the objects in the list to be synchronized from the master vGW Security Design VM to the delegate center that you are defining.
 - **Global Policy**—Synchronizes the global policy and all objects it depends on. Among other objects, configurations for the source and destination of the rules in the policy and the protocols are copied.

- **Default Policy**—Synchronizes the default policy and all objects it depends on. Among other objects, configurations for the source and destination of the rules in the policy and the protocols are copied.
- **Quarantine Policy**—Synchronizes the quarantine policy and all objects it depends on. Among other objects, configurations for the source and destination of the rules in the policy and the protocols are copied.
- **Policy Groups**—Synchronizes all the policy groups and policies associated with them, and all objects that they depend on. Among other configurations, the sources and destinations of the rules in the policies, the protocols, the networks and the machines in the groups are copied.
- **Monitoring Groups**—Synchronizes all the monitoring groups and the policies associated with them, and all objects that they depend on. Among other configurations, the sources and destinations of the rules in the policies, the protocols, the networks and the machines in the groups are copied.
- **Networks**—Synchronizes all networks.
- **External Machines**—Synchronizes all external machines.
- **IDS Signatures**—Synchronizes IDS Signatures and Settings.
- **Compliance**—Synchronizes compliance rules and all objects that they depend on, such as groups.
- **Antivirus Settings**—Synchronizes all AntiVirus scan configurations, and all objects that they depend, such as groups.

Configuring Split-Center and Multi-Center for vGW Security Design VMs

Configuring Split-Center for the First vGW Security Design VM

Step-by-Step Procedure This configuration shows how to use the Split-Center feature to give vGW Security Design VM-1 management responsibility for part of the resources at vCenter1.

From the Settings module **vGW Application Settings > vCenter Integration** page:

1. In the vCenter Settings pane, enter the following information:
 - The server name or IP address of the vCenter. For this example, enter **vCenter1**.
 - The vGW Security Design VM-1 username and password to authenticate to vCenter1. For this example, enter **admin-1** and **talk#321**.
2. In the vCenter Settings pane, select a management scope for vGW Security Design VM-1. To display the data centers belonging to vCenter1, select the **Selected Datacenters** option button.

The data centers belonging to vCenter1 are displayed:

- vCenter1-data-center-1
- vCenter1-data-center-2
- vCenter1-data-center-3

- vCenter1-data-center-4
- vCenter1-data-center-5

By default, the system is configured to allow the vGW Security Design VM to manage all data centers.

3. Click the check box before vCenter1-data-center-1, and click **Save** to allow vGW Security Design VM-1 to manage it.

vGW Security Design VM-1 will now be able to manage only the VMs and other resources for vCenter1-data-center-1 of vCenter1.



NOTE: Before the system saves your selection, vCenter1 verifies the authentication credentials that you specified. The system displays the following message:

Checking vCenter login credentials. This may take up to 15 seconds depending on server loads.

If your credentials are invalid, your data center scope management selection is not committed.

4. If you want to commit the configuration, click **Okay**.

Configuring Split-Center for the Second vGW Security Design VM

Step-by-Step Procedure

This configuration shows how to use the Split-Center feature to give vGW Security Design VM-2 management responsibility for part of the resources at vCenter1.

1. From vGW Security Design VM-2, select the Settings module.
2. In the navigation tree, select vCenter Integration beneath vGW Application Settings.
3. In the vCenter Settings pane, enter the following information:
 - The server name or IP address of the vCenter. For this example, enter **vCenter1**.
 - The vGW Security Design VM-2 username and password to authenticate to vCenter1. For this example, enter **admin-2** and **talk#4*5#6**.
4. In the vCenter Settings pane, select a management scope for vGW Security Design VM-2. To display the data centers belonging to vCenter1, select the **Selected Data centers** option button.

The data centers belonging to vCenter1 are displayed:

- vCenter1-data-center-1
- vCenter1-data-center-2
- vCenter1-data-center-3

- vCenter1-data-center-4
- vCenter1-data-center-5

By default, the system is configured to allow the vGW Security Design VM to manage all data centers.

5. Click the check boxes before vCenter1-data-center-2, vCenter1-data-center-3, vCenter1-data-center-4, vCenter1-data-center-5, and click **Save** to allow vGW Security Design VM-2 to manage them.



.....

NOTE: Before the system saves your selection, vCenter1 verifies the authentication credentials that you specified. The system displays the following message:

Checking vCenter login credentials. This may take up to 15 seconds depending on server loads.

If your credentials are invalid, your data center scope management selection is not committed.

.....

6. To commit the configuration, click **Okay**.

Defining Entries for a Delegate Center Using the Multi-Center Feature

Step-by-Step Procedure

This example shows how to define entries for one of the three vGW Security Design VMs to allow it to become a delegate center and inherit most of the vGW Security Design VM-3 master's configuration. Configuration of the other two delegate centers is not shown here, but it is done similarly to the single configuration example.

This example shows how to configure:

- Entries for vGW Security Design VM-1 and vGW Security Design VM-2 to allow all configuration objects to be copied to them.
- An entry for vGW Security Design VM-4 to allow all configuration objects excluding monitoring groups and IDS to be copied to it.

To define a delegate center entry for vGW Security Design VM-1, from the vGW Security Design VM-3 master Settings module **vGW Application Settings > Multi-Center** page:

1. Enter **mc-delegate-1** as the name for the delegate center entry.
2. Enter **admin-1** and **talk#321** as the user ID and password credentials of the delegate center.
3. Under Synchronize Objects, click **Select All**.
4. If you are satisfied with the configuration, click **Save**. Otherwise, click **Cancel**.

- Related Documentation**
- *Understanding vGW Series*
 - [Understanding the Multi-Center Feature on page 63](#)
 - [Understanding vGW Series Multi-Center Synchronized Objects on page 69](#)

CHAPTER 7

Administrators Definitions and Permissions

- [Adding New vGW Series Administrator Definitions, Permissions, and Authorization Using the Settings Module on page 79](#)
- [Setting Up Active Directory for vGW Series Administrator Authentication on page 83](#)

Adding New vGW Series Administrator Definitions, Permissions, and Authorization Using the Settings Module

Different categories of IT staff members may need to access the vGW Security Design VM interface for various purposes. For example, network engineers can take advantage of the network statistics charts and information on connections, top protocols used, top sources, and top destinations. Security engineers can use the Firewall module to design and apply policies for VMs and the Settings module's vGW Application Settings > Installation page to deploy vGW Security VMs to ESX/ESXi hosts to secure them.

[Table 4 on page 79](#) defines the built-in user types that vGW Series provides to accommodate common roles and requirements, and it describes their privileges.

Table 4: vGW Series Built-In Administrator User Types

Global Admin	<p>This administrator has the highest level of system privileges, including the ability to create accounts for additional administrators.</p> <p>The global administrator has many privileges including:</p> <ul style="list-style-type: none">• creating firewall policies and installing firewalls (vGW Security VMs) on ESX/ESXi hosts to be secured.• configuring features such AntiVirus, IDS, and VM Introspection Compliance for VMs.• selecting port groups and VMs for insertion in and removal from a secured network. <p>This administrator can also reset his own password and that of another of administrator account. Having the ability to reset the password for another administrator is useful when an administrator forgets his password. For details see</p>
--------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Table 4: vGW Series Built-In Administrator User Types (*continued*)

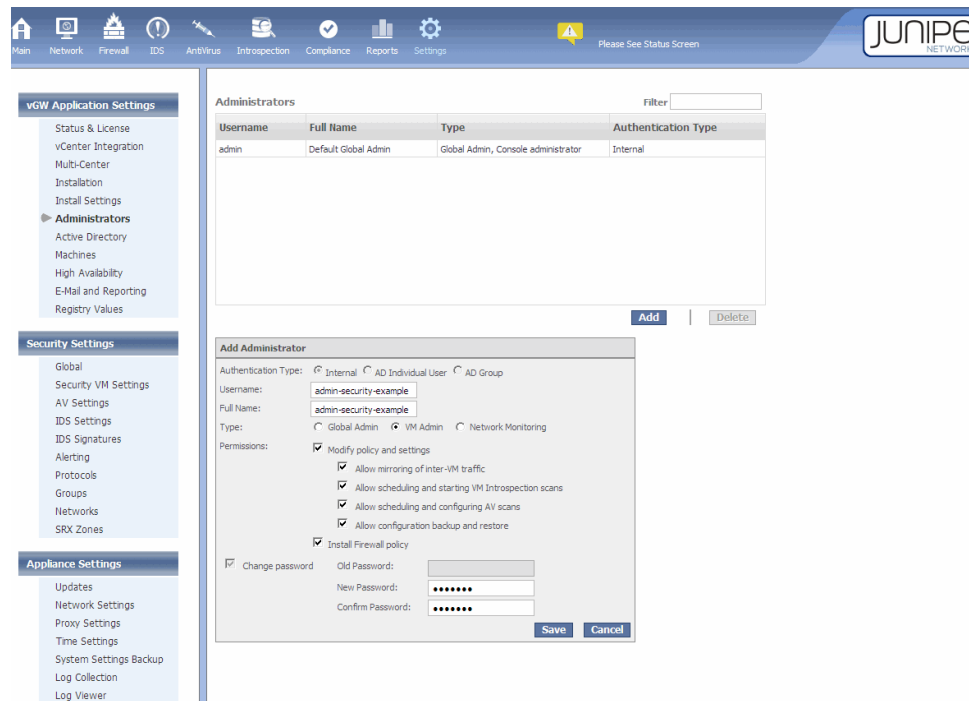
VM Admin	<p>These administrators have many privileges, including the ability to:</p> <ul style="list-style-type: none">• modify policies and configuration of settings. The administrator is allowed to change firewall security policies, including IDS.• configure AntiVirus and VM Introspection Compliance.• configure mirroring of inter-vm traffic, the ability to configure rules to specify external inspection devices. <p>Additionally, the global administrator can grant VM Admins "Install Firewall Policy" privilege. This privilege allows a VM Admin to distribute a policy after it has been changed and saved by any administrator who has the privilege to modify security policies.</p>
Network Monitoring	<p>These administrators can view:</p> <ul style="list-style-type: none">• all network-related pages, for example pages that show statistics and graphs.• all tabs of the Main module, including Status and Events and Alerts, and Logs. <p>These administrators are not allowed to modify any Settings pages, but they can view IDS Alerts, if IDS is configured, view AntiVirus scans, and they can view but not modify VM Introspection and Compliance results.</p>

To create an administrator account:

1. From Settings module vGW Application Settings > Administrators page, click **Add**.

Figure 20 on page 81 shows the Administrators page > Add Administrator pane that you use to define permissions for a new administrator and add the administrator to the system. This configuration specifies that authentication is performed internally by vGW Series, not by Active Directory (AD) which can also be used. In this example, the VM Admin admin-security-example administrator is allowed to modify policy and settings and push firewall policies to vGW Security VMs.

Figure 20: Creating a VM Admin Administrator Account



2. In the **Authentication Type:** area, select the radio button associated with the kind of authentication to be used for this administrator. For details on AD authentication, see [“Setting Up Active Directory for vGW Series Administrator Authentication” on page 83](#).
3. In the **Username:** and **Full Name:** fields, enter the user names for the administrator.
4. In the **Type:** area, select the radio button associated with the type of administrator account that you want to create. See [Table 4 on page 79](#).
5. In the Permissions: area select the permissions that you want to grant to the administrator. Notice that for VM Admin you can select “Modify policy and settings” and “Install Firewall policy”, but if you select Network Monitoring you cannot select any of these permissions. See [Table 4 on page 79](#) for allowed permissions.
6. Specify a password and confirm the password.
7. Click **Save**.

After you save the configuration, the administrator definition is added to the Administrators table, as shown in [Figure 21 on page 82](#).

Figure 21: Adding a New Administrator

Administrators Filter

Username	Full Name	Type	Authentication Type
admin	Default Global Admin	Global Admin, Console administrator	Internal
admin-security-examp	admin-security-example	VM Admin	Internal

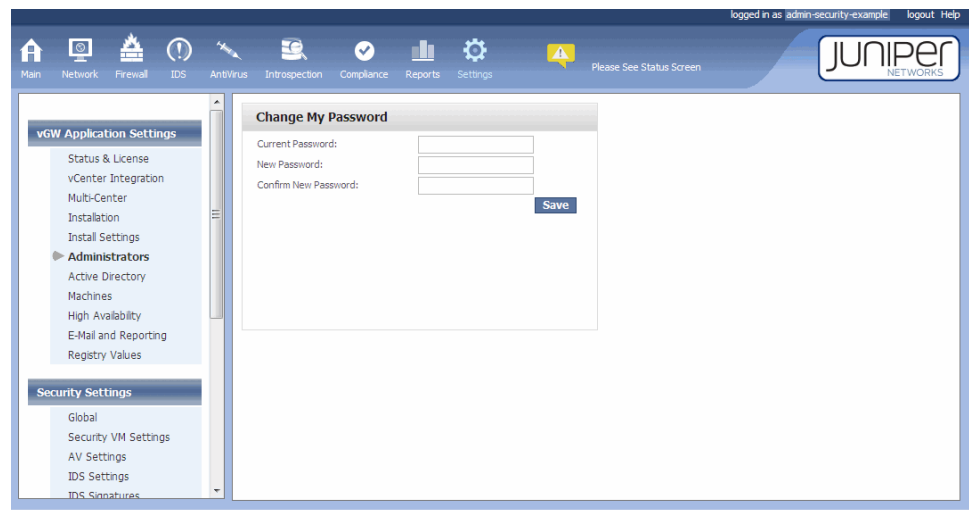


NOTE: At any time, you can click the table row for an administrator definition to display the Edit Administrator pane that shows the configuration. From the Edit Administrator pane you can modify the permissions and password and save the modified definition.

When Global Admin users are logged into the vGW Security Design VM and they select the Settings module vGW Application Settings > Administrators page, the Add Administrator pane shown in [Figure 20 on page 81](#) is displayed. It allows them to add new administrators.

When other administrators select the Settings module vGW Application Settings > Administrators, the Change My Password dialog box, shown in [Figure 22 on page 83](#), is displayed. This dialog box allows the administrator to enter a new password. However, the administrator must enter their current password before they are allowed to change it to the new one. After the administrator clicks **Save**, vGW Series verifies the current password. If it is valid, it changes the current password to the new password.

Figure 22: Changing the Password for a Defined Administrator



Related Documentation

- *Understanding vGW Series*
- [Setting Up Active Directory for vGW Series Administrator Authentication on page 83](#)
- *Configuring vGW Series Firewall Policies*
- *Understanding the vGW Security VM*
- *Understanding the vGW Security Design VM*

Setting Up Active Directory for vGW Series Administrator Authentication

This topic covers use of Active Directory (AD) for administrator authentication. First it explains how to enable AD support for vGW Series, which you must do before you can configure administrator authentication to use it. Then it explains how to configure it as the authentication type for an administrator.

You can use AD with vGW Series for administrator authentication instead of storing the authentication information locally in the vGW Security Design VM database. vGW Series supports AD over IPv4 and IPv6 networks.

Administrators can use their AD credentials to log in to the vGW Security Design VM. vGW Series checks AD for the credentials, and, based on the settings, it allows the user to log in to vGW Security Design VM or it denies the user access.

To set up the vGW Series to work with AD:

1. Define the Name (or IP address) of the AD server on the Active Directory configuration page.
2. Set the appropriate port. By default, port TCP 636 (LDAPS) is used. However, you can use 389 LDAP+STARTTLS or configure a custom port.

Enable your network to give the vGW Security Design VM access to this port to the server.

3. After you select the name or IP address, port, and default search base, select **Test** or **Save** to view the fingerprint used to validate the communication destination and to initiate all future communication through encryption.

When you select **AD Group** for **Authentication type**, a dialog box is displayed allowing you to enter the user ID and password to use to log in to AD to get the group list.



NOTE: AD must be enabled for you to select **AD Group** as the authentication method. Use the Settings module **vGW Application Settings > Active Directory** page to enable it, as described previously.

If there are more than 100 configurable groups, vGW Series presents the following alert message:

"There are too many groups in Active Directory to be displayed in a drop-down list. Please fill in the name of the AD Group."

Rather than displaying a drop-down list of group names, the AD Group Name field is presented as a text box in which you can enter the name of the group.

When you save the configuration, vGW Series checks AD to ensure that the group exists, based on the name that you entered. If the group does not exist, vGW Series displays the following message:

"The AD Group *name* does not exist in Active Directory."

To create users or groups to be authenticated through the configured server lookup process:

1. Select the Settings module > vGW Application Settings > Administrators page.
2. Add administrators. Set the authentication type to **AD Individual User** or **AD Group**.
 - For AD Individual User, the account is authenticated with AD credentials and all privileges are applied according to defined vGW Series settings.
 - For AD Group, the name of an existing group in AD is used and privileges are assigned to it. The AD lookup is used to authenticate the user to determine that he is a member of the group. If so, he is granted access to vGW Series.

**Related
Documentation**

- *Adding New vGW Series Administrator Definitions, Permissions, and Authentication Using the Settings Module*
- *Understanding vGW Series*
- *Configuring vGW Series Firewall Policies*
- *Understanding the vGW Security VM*
- *Understanding the vGW Security Design VM*
- [Adding and Editing vGW Series Machines Definitions \(VMware\) on page 85](#)

CHAPTER 8

Machine Definitions for VMs and Other Resources

- [Adding and Editing vGW Series Machines Definitions \(VMware\) on page 85](#)

Adding and Editing vGW Series Machines Definitions (VMware)

This topic covers the Machines page that you use to define IP addresses and other information for new machines. These machines include both VMware ESX/ESXi hosts and virtual machines (VMs) that you define for your environment. You also use this page to view or edit information about machines that are already defined, including those that are discovered automatically. Machines can have IPv4 or IPv6 addresses.

This topic describes a new parameter provided with vGW Series Release 5.5—Log Tags—that allows you to specify tags that are added to syslog output. You can use these tags to sort on syslog feed.

This topic includes the following sections:

- [Adding a Machine on page 85](#)
- [Viewing Machine Information on page 87](#)

Adding a Machine

Normally the IP address for a machine is “auto-discovered”, obtained through VMware Tools. For systems without VMware Tools, you can use the Settings module Applications Settings > Machines page to manually add addressing information for a machine. You can also specify additional information for a machine, such as Log Tags and Smart Tags.

To configure information for a machine, enter:

- **Name:** This is the name of the machine (VM). By default, it is set to synchronize with the VMware vCenter. However, you can detach it by clearing the Synchronize name with vCenter checkbox.

In Release 5.5, vGW Series adds the name to syslog output, instead of adding just VM_ID. The name is relative to the VM that is either the source (src) or destination (dst) of the log flow. For example, dst_name="mini-5-1" or src_name="mini-5-1". hr".

- **Description:** Give a brief description of the machine.

- For the machine's address, use DNS for the machine name or enter its address explicitly.

- **DNS name:**

If you define a machine in this section, it is identified in the network tables by its name rather than by its IP address.

- Specify the machine's DNS name.
- To obtain the name through a DNS query, click **Query via DNS**.

- **IP Address:** Specify the machine's IP address explicitly.

- **Smart Tags:** Optionally, configure Smart Tags to assign identifiers to the machine that can be used for VM Smart Groups or policy creation.

The syntax for a Smart Tag is attribute-value. You can define multiple tags separated by semicolons, for example: finance;pci=true;audited=true.

- **Log Tags:** Optionally, specify Log Tags to be added to Syslog entries for this machine.

In conjunction with the VM name that is added to Syslogs as of vGW Series Release 5.5, this option allows you to specify any tag that you want to use to be added to the syslogs. For example, you can use this tag to associate certain VMs with a Tenant or Department such as customer A's VMs are tagged with 'cust-a' and which are then sorted automatically from the syslog feed by parsing on this tag.

Similar to the VM name tag described above, these tags are relevant on direction of the flow (src_log_tag or dst_log_tag). For example, dst_log_tag="testLogTags". These logs are issued when vGW Series processes secured VM traffic or files.

The Log Tag string pertains to this VM only. It cannot exceed 200 characters. Figure [Figure 23 on page 87](#) shows the edit screen that includes a log tag for a machine that was already added. Figure [Figure 24 on page 87](#) shows the resulting syslog entry.

The Log Tag string pertains to this VM only. It cannot exceed 200 characters.

- **Type:** This is the type of machine, for example, ESX/ESXi server, external machine
- **Monitoring Groups:** Monitoring groups that the machine belongs to.
- **Policy Groups:** Policy Groups that the machine belongs to.
- **VMSafe Protected:** Whether the machine is secured by vGW Series.

When you select a VM, as opposed to an ESX/ESXi server, and display the Edit Machine box for it, this information is displayed for it.



NOTE: If you click **Advanced**... You can change the behavior if vGW Series fails to connect to the kernel (failopen or failclosed).

You can also use the Machines page to edit information for an existing machine. See [Figure 23 on page 87](#).

Figure 23: Configuring Machines Information

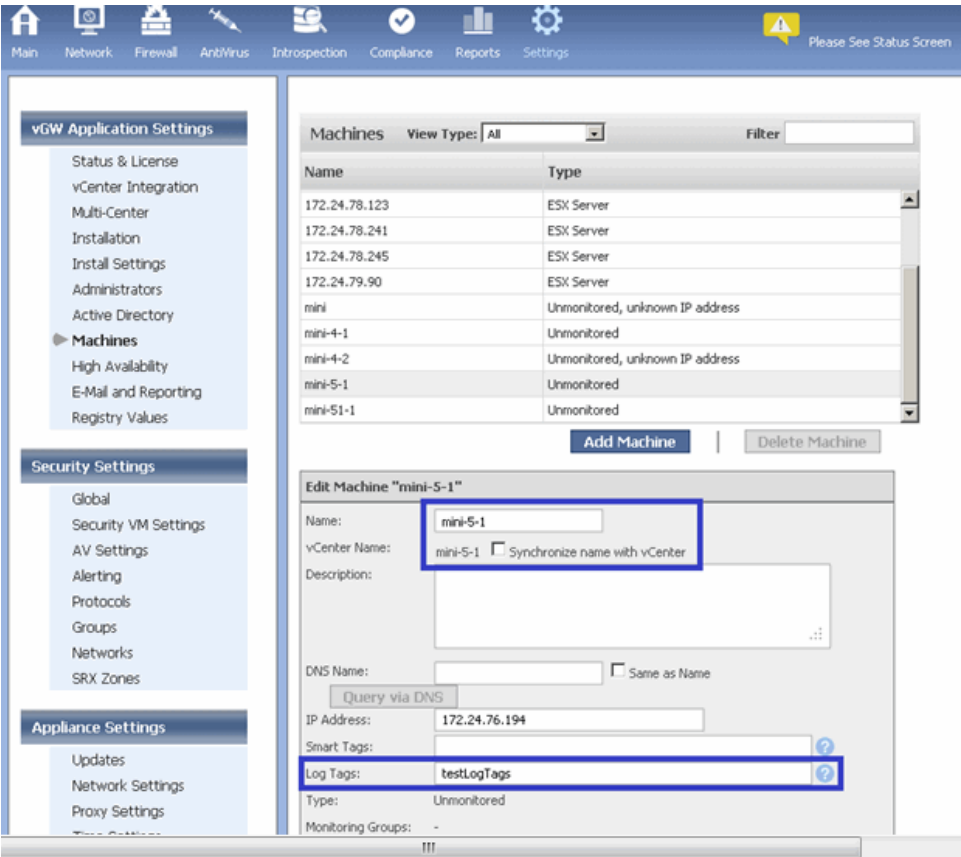
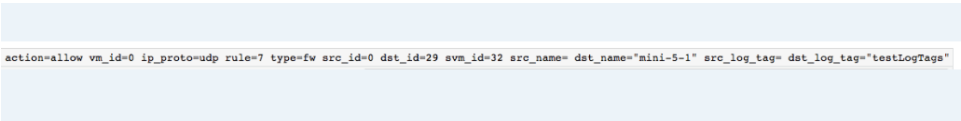


Figure 24: Syslog Entry Including VM Name and Log Tag



Viewing Machine Information

You can view information about machines that are already defined. You can use the **View Type:** box to sort the list by machine type. You can sort by ESX servers, external machines, monitored, unmonitored, and secured machines.

You can use the Filter box to search by a portion of an IP address or machine name or type.

- Related Documentation
- *Understanding vGW Series*
 - *vGW Security Design VM Modules (VMware)*

CHAPTER 9

E-Mail and Reporting

- [Configuring vGW Series E-Mail and Reporting Applications Settings on page 89](#)

Configuring vGW Series E-Mail and Reporting Applications Settings

You use the Settings module vGW Application Settings E-Mail and Reporting section to configure the e-mail server and account information. This information is used throughout vGW Series for distributing status and log messages and reports.

During the installation of the vGW Security Design VM, you can configure the parameters required to generate automated reports.

To configure or change these parameters, use the Settings module > vGW Application Settings > E-Mail and Reporting page, and enter the new values.

The following list describes the e-mail settings and configuration parameters:

SMTP Server—Hostname or IP address where e-mail is sent. You can specify either a valid IPv4 address or IPv6 address.

SMTP Port—Port used by the mail server (common values are 25 or 465 for encrypted).

Authenticate—If authentication to the mail server is required, check this option.

TLS Authenticate—If the mail server uses TLS encryption, select this option.

SMTP—If authentication is required, use this user account.

E-mail From—Text that appears in the From field in e-mail messages.

E-mail To—Text that appears in the To field in e-mail messages.



TIP: You can troubleshoot mail server configuration errors by clicking **Test Mail Server** before saving parameter changes.

The reporting module settings configuration parameters are:

Default e-mail From—Text that will appear in the From field of e-mail messages by default.

Mail Subject —Text you want inserted in the Subject line for messages sent by the Reporting module.

Mail Content —Text you want inserted in the content section of messages. (The report itself is attached as a PDF file.)

**Related
Documentation**

- *Understanding vGW Series*
- *Understanding the vGW Security Design VM*
- *Understanding the vGW Security VM*

PART 3

Security Settings

- [Getting Started on page 93](#)
- [Antivirus and IDS Settings on page 103](#)
- [Groups on page 111](#)
- [Alerts on page 127](#)
- [SRX Series Devices on page 129](#)
- [Networks and Protocols on page 131](#)

CHAPTER 10

Getting Started

- [Understanding the vGW Series Security Settings on page 93](#)
- [Configuring Global Settings Using the vGW Series Settings Module on page 94](#)
- [Understanding the vGW Security VM Settings on page 97](#)

Understanding the vGW Series Security Settings

The Settings module Security Settings section controls the core vGW Series functions. The Security Settings module brings together configuration of many parts of your deployment so that you can configure or change them in one place.

The Settings Module > Security Settings includes the following sections:

- Global
See [Configuring Global Settings Using the vGW Series Settings Module \(VMware\)](#).
- Security VM Settings
See [“Understanding the vGW Security VM Settings” on page 97](#).
- AV Settings
See [“Understanding and Configuring the vGW Series AntiVirus Settings” on page 103](#)
- IDS Configuration
See [“Understanding and Configuring IDS Settings” on page 104](#).
- IDS Signatures
See [“Understanding and Configuring IDS Settings” on page 104](#).
- Alerting
See [“Understanding the vGW Series Security Alert Settings” on page 127](#).
- Protocols
See [Understanding vGW Series Protocols Support](#)
- Groups
See [“Understanding vGW Series Groups” on page 111](#).
- Networks

See [“Understanding the Settings Module Networks Settings”](#) on page 131.

- SRX Zones

See *vGW Series and SRX Series Security Zones*.

**Related
Documentation**

- *Understanding vGW Series*
- *Understanding the vGW Security Design VM*

Configuring Global Settings Using the vGW Series Settings Module

The Security Settings > Global Settings page of the vGW Security Design VM allows you to identify the external inspection devices to send traffic to for further analysis, the Syslog server to use for external logging, global settings rules, and NetFlow configuration information identifying where to send connection flow data. This topic addresses how to configure this information and other related global settings. The topic also covers vGW Series support of IPv6 in relation to global settings.



BEST PRACTICE: You can easily avoid any potential problems mentioned in this topic by using the Security Settings > Security VM Settings page to configure locations of servers for individual vGW Security VMs. For example, if the vGW Security VM has an IPv6 address, configure servers with IPv6 addresses for it. If the vGW Security VM has an IPv4 address, configure servers with IPv4 addresses. [Figure 25 on page 95](#) shows the vGW Security Design VM Global Settings page.

Figure 25: Configuring vGW Series Global Settings

The screenshot shows the Juniper vGW Series Global Settings configuration page. The top navigation bar includes links for Main, Network, Firewall, IDS, AntiVirus, Intrusion, Compliance, Reports, and Settings. The user is logged in as 'Demo User'. The left sidebar contains a tree view of settings categories: vGW Application Settings, Security Settings, and Appliance Settings. The main content area is divided into five sections:

- External Inspection Devices:** Configure the names and IP addresses for external content inspection devices. A table lists 4 devices with columns for Name and IP Address. The first device is 'Juniper IDP' with IP '192.168.0.1'. A 'Save' button is at the bottom.
- External Logging:** External logging will send logs to external server using syslog. Options include: No Syslog (selected), Send Syslog from vGW management server, Send Syslog from Firewalls, and Send firewall logs to vGW management server. Fields for Syslog Server and Syslog Server Port (514) are provided. A 'Save' button is at the bottom.
- Global Settings Rules:** Allow or drop specific types of traffic for all VMs, and enable or disable logging for the rules. A table lists 4 rules with columns for Rule, Allow, and Log. Rule 1 is 'IPv6 traffic', Rule 2 is 'Non-IP and non-ARP traffic', Rule 3 is 'Multicast traffic', and Rule 4 is 'Broadcast traffic'. A 'Save' button is at the bottom.
- NetFlow Configuration:** Send records to NetFlow collector. An 'Enable' checkbox is present. Fields for NetFlow collector address and NetFlow collector port (2055) are provided. A 'Save' button is at the bottom.
- Infrastructure Configuration Enforcement:** vGW monitors the VMs' control network to ensure no other VMs are connected to this network. If a new VM is connected to this network, what action should be taken? Options include: Disconnect the VM's virtual network interface (selected), Generate an alert to the Security Design vGW administrator, and Ignore this event. A 'Save' button is at the bottom.

Global settings take effect for all vGW Security VMs that you installed using the vGW Security Design VM *unless* you use the Security Settings > Security VM Settings page to configure different devices for a particular vGW Security VM to use.

vGW Series supports both IPv4 and IPv6 addresses, including support for vGW Security VMs with different IP protocol version addresses configured using the same vGW Security Design VM.



NOTE: If a server is identified by its DNS name, the vGW Security VMs will connect and send information to the correct, resolved address: vGW Security VMs with IPv4 addresses will send data to the matching A record and vGW Security VMs with IPv6 addresses will send data to the matching AAAA record.

vGW Security VMs that you configure could have associated with them addresses that belong to different IP protocol versions. Some vGW Security VMs might be assigned IPv4 addresses while others might be assigned IPv6 addresses. For example, vgw-svm12 might be assigned the IPv4 address 116.27.61.137 while vgw-svm13 might be assigned the IPv6 address 2001:cdba::3257:9653.

It might be the case that addresses assigned to Syslog, GRE, or Netflow servers and the vGW Security VMs that need to connect to them to send data belong to different IP

protocol versions. For example, syslog-server-1 might be assigned the IPv6 address FE80::0202:B3FF:FE1E:8329 whereas vgw-svm12 might be assigned the IPv4 address 116.27.61.137.

In cases where the IP protocol versions differ, the following results take effect:

- vGW Series issues the following message to alert you to the fact that a particular vGW Security VM is not able to connect to the device whose IP protocol version address differs from its own.
- The vGW Security VM does not send out traffic to that server.

For example, if syslog-server-1 is assigned to the IPv6 address FE80::0202:B3FF:FE1E:8329 and vGW Security Design VM vgw-svm12 is assigned an IPv4 address 116.27.61.137, vgw-svm1 will not send Syslog messages to syslog-server-1.

- If in the Global Settings page External Logging pane the checkbox “Send firewall logs to the vGW management center” is selected, the vGW Security VMs send Syslog messages to the vGW Security Design VM. This behavior applies regardless of whether the IP protocol versions of the vGW Security VM and the Syslog server match. The Syslog server address has no bearing on sending the logs to the vGW Security Design VM.

However, if you clear this check box at the Security Settings > Security VM Settings page for a particular vGW Security VM, then that vGW Security VM will not send logs to the vGW Security Design VM.

The Global settings page contains the following panes:

- External Inspection Devices—This pane allows you to enter the names and IP addresses of devices to which traffic can be sent for further analysis such as Intrusion Detection Systems and Network Analyzers. The external inspection device must be capable of terminating a GRE tunnel. The vGW Security VM is the source of the traffic. For traffic to be sent, you must configure a policy rule. Real-time packet flows encapsulated in GRE are sent to the destination IP address that you specify based on the appropriate rule. Traffic matching the policy rule is sent to the destination IP address that you define for this parameter.

The configuration mirrors the traffic to the external device—it does not imply that traffic is accepted or rejected. You must decide whether to accept or reject the traffic in subsequent rules in the policy. Mirrored traffic shows up in logs if logs is also configured with **duplicate** in the action field.

vGW Series supports both IPv4 and IPv6 addresses. If one or more of the vGW Security VMs configured on the vGW Security Design VM has associated with it an address type that is different from the type of address assigned to the external inspection device, vGW Series issues an alert to inform you that the vGW Security VM in question cannot connect to the external inspection device.

You can use third-party products by creating different rules for the type of traffic you want inspected and redirected.

- Global Settings Rules—You can configure the vGW Security VM firewall to deal with four types of traffic in different ways. The default firewall configuration drops IPv6 and

non-IP traffic, such as IPX. Multicast and Broadcast can be globally allowed (default) or dropped as configured in this pane (with the option to log the traffic). The multicast logging option does not hide the log traffic from the graphs. This setting controls whether the traffic creates connection logs in the Logs view.

- **External Logging**—The vGW Series supports sending logs to third-party Syslog servers. You can enable or disable the feature in this pane. If it is enabled, all traffic that matches a log firewall rule is written to the vGW Series logs. It is also written to the destination Syslog server. You can also customize the Syslog format .



TIP: You can override the global configuration for an individual vGW Security VM for a host using the Settings module, Security VMs section.

- **NetFlow Configuration**—You can specify that all connection flow information is sent through NetFlow Version 9 by enabling the setting in this pane, and selecting an IP address and a port. Ports 2055 and 9990-9999 are commonly used. Both NetFlow and Syslog are compatible with Juniper Networks STRM.



TIP: You can override the configuration through the individual vGW Security VM for the host using the Settings module, Security VMs section.

- **Infrastructure Configuration Enforcement**—VMware requires a special network for communication between the vGW Security VM and VMsafe. This network should not have guest VMs (VM) connected to it that are not part of the VMsafe communication process. If someone connects a VM to this network, this option allows you to disconnect the VM for heightened security.

Related Documentation

- *Understanding vGW Series*

Understanding the vGW Security VM Settings

The Settings module Security Settings > Security VM Settings page allows you to view in one place settings configured for each deployed vGW Security VM. From this page, you can select an individual vGW Security VM and change its configuration, configure a secondary vGW Security VM for it for high availability, and override global settings.



TIP: You can also navigate to this page from the Status section of the Main module. To do so, in the Main module Status page > Status of Security VMs pane, click the row for the vGW Security VM whose configuration you want to view or configure.

The Security VMs pane at the top of the page includes a table with a row for each deployed vGW Security VM, showing the following information:

- Address of the ESX/ESXi host it is deployed to
- Number of VMs that it protects
- If high availability is configured for it
- If network monitoring is enabled
- If NetFlow is configured
- If Syslog is configured
- AntiVirus signature version and data base configuration
- Version of the vGW Security VM

To display a pane that allows you to see detailed information about a vGW Security VM configuration and re-configure its settings, click the vGW Security VM's row.

You can use the tabs shown in the displayed pane to configure unique settings for the vGW Security VM that override the global settings or those set for it when it was installed.

- **VM Settings**—This tab displays configuration information for the vGW Security VM that was set when the vGW Security VM was installed or last modified, in particular the type of IP address assigned to it and how it is obtained. [Figure 26 on page 98](#) shows the pane that you use to change the IP addresses for the vGW Security VM management interface that it uses to communicate with the vGW Security Design VM interface. You can use this pane to override the addresses that were set when you installed the vGW Security VM.

This pane allows you to change the IP protocol family that is used for the vGW Security VM management interface when that protocol does not match that of the vGW Security Design VM with which it must communicate. For information on conditions that would cause an IP address type mismatch between the management interfaces of the vGW Security VM and the vGW Security Design VM, see *Setting Up vGW Series* and [“Installing vGW Security VMs on ESX/ESXi Hosts” on page 15](#).

Figure 26: Changing the vGW Security VM Management Interface IP Address

The screenshot shows the 'VM Settings' tab selected. The 'Security VM IP Configuration' section is active, displaying a form to change the IP configuration. The 'Internet Protocol' section has two dropdowns: 'IPv4' set to 'DHCP' and 'IPv6' set to 'DHCPv6'. Below these are input fields for 'IP Address', 'Netmask', and 'Default Gateway'. The 'Netmask' field has a 'prefix' label. An 'Update' button is at the bottom right of the form. To the right, the 'High Availability' section is visible with a 'Configure' button.

You can change the settings for:

- **IPv4:**

For IPv4, from the displayed list, select the method to use to assign an IPv4 address to Interface 1:

- **DHCP**

Use a DHCP server to assign dynamically an IPv4 address to Interface 1. This is the default method. However, this tab page will reflect the configuration set for this vGW Security VM when it was installed or last modified.

- **Static IP**

Specify a static IP address and its network mask routing prefix, and the default gateway to assign to Interface 1.

- **IPv6:**

For IPv6, from the displayed list, select the method to use to assign an IPv6 address to Interface 1:

- **DHCPv6**

Use a DHCPv6 server to obtain the IPv6 address for Interface 1. This is the default method. However, this tab page will reflect the configuration set for this vGW Security VM when it was installed or last modified.

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to IPv6 stateless address autoconfiguration.

- **Autoconfiguration**

Use stateless address autoconfiguration to obtain the IPv6 address for Interface 1. IPv6 stateless address autoconfiguration allows network devices attached to an IPv6 network to automatically acquire IP addresses and connect to the Internet without intermediate interaction with a DHCPv6 server.

Refer to *RFC 2462, IPv6 Stateless Address Autoconfiguration* for details.

- **Static IP**

Specify a static IP address for Interface 1 including the IPv6 address prefix (the initial bits of the address that denote the network address, akin to a netmask) and the default gateway to use for it.

- **Network Monitoring**—This tab displays Network traffic monitoring, console monitoring, and NetFlow configuration information.

- **Network Traffic Monitoring**—By default, network traffic monitoring data is sent to the vGW Security Design VM from all vGW Security VMs. In most cases, it is useful to collect network traffic information that is then displayed in the vGW Series Network module. If you are interested in implementing only firewall protection for VMs protected by this vGW Security VM, you can increase overall system performance by disabling network monitoring on this page. If this option remains enabled for other vGW Security VMs, they will continue to collect and display traffic statistics in the Network module pages.

- **Console Monitoring**—You can turn console monitoring on or off. Turning it on directs vGW Series to connect to the hypervisor console to monitor traffic in and out of the system to ensure that inappropriate activity is not occurring.
- **Off**—No monitoring is performed.
- **Monitor**—Network traffic to the hypervisor console (management center) vNIC is monitored by vGW Series Network module. If netflow is enabled, network traffic information is also available as netflow data.

See [Figure 27 on page 100](#).

Figure 27: Configuring the Security VM Settings Page Console Monitoring

Virtual Switch	VMKernel Port	Monitoring Port Group	VLAN Id	Distributed Virtual Switch
<input checked="" type="checkbox"/> vSwitch0	--Management Network		4095	false

In addition to monitoring activity as described previously, you can enable IDS traffic monitoring for the vGW Security VM. In this case, network traffic is mirrored to the IDS engine. IDS flags any suspicious activity with high, medium, or low priority alerts, based on how you configured it. For details on IDS, see *Understanding the vGW Series IDS Module* and related topics.

To enable IDS monitoring, you must use the IDS tab. If IDS is enabled for the vGW Security VM, the message “IDS inspection console is enabled, see IDS tab.” is displayed in the Console Monitoring box. This message does not appear unless you have enabled IDS.

- **NetFlow Configuration**—You can enable or disable NetFlow for the vGW Security VM. (You cannot change these settings unless NetFlow is enabled globally.)



NOTE: The NetFlow server must be routable from the vGW Security VM.

If NetFlow is enabled, you can direct the vGW Series to send NetFlow data from this vGW Security VM to a different NetFlow collector than the one that is specified in the Settings module’s Global section.

To send records to a different NetFlow connector:

1. Select **Enable**.
2. Select **Override global netflow configuration**.
3. Specify the NetFlow collector’s address information.

vGW Series supports IPv4 and IPv6 addresses.

4. Click **Save**.

See [Figure 28 on page 101](#).

Figure 28: Configuring Network Monitoring for Individual vGW Security VMs

The screenshot displays the 'Network Monitoring' tab within the vGW Security VM configuration window. The window has a top navigation bar with tabs: VM Settings, Network Monitoring (selected), IDS, Syslog, AntiVirus, Updates, and Support. A 'Close' button is in the top right corner. The 'Network Monitoring' section contains three sub-panels:

- Network Traffic Monitoring:** Includes the instruction 'Enable traffic monitoring.' and a checked checkbox labeled 'Enable'. A 'Save' button is at the bottom right.
- Console Monitoring:** Includes the instruction 'Monitor hypervisor console communication.' and two radio buttons: 'Off' (selected) and 'Monitor'. A 'Save' button is at the bottom right.
- NetFlow Configuration:** Includes the instruction 'Send records to NetFlow collector.' and two unchecked checkboxes: 'Enable' and 'Override global netflow configuration'. Below these is a text field for 'NetFlow collector address:' followed by a 'Save' button.

- **IDS**—This tab allows you to enable or disable the IDS engine for the vGW Security VM. If IDS is disabled, you must first enable it globally before you can enable it for the vGW Security VM. You can also turn on IDS inspection of the console by selecting **Enable IDS inspection on the console**.

For details on enabling IDS globally, see *Configuring Global Settings Using the vGW Series Settings Module (VMware)*.

- **Syslog**—This tab allows you to define a Syslog server to use for this vGW Security VM. vGW Series supports sending logs to third-party Syslog servers. To override the Global syslog configuration and specify a different syslog server to use for this vGW Security VM.
 1. Select **Override global syslog configuration**.
 2. Specify the IP address, the port, and the transport protocol of the Syslog server to use for this vGW Security VM.
 3. Click **Save**.
- **AntiVirus**—This tab allows you to enable or disable vGW AntiVirus for this vGW Security VM. If you do not want all ESX/ESXi hosts that are protected by vGW Series to have vGW AntiVirus protection, you can use this page to disable it for the individual vGW Security VM that protects the intended ESX/ESXi host.

- Updates—You can use this tab to update the vGW Security VM. For details on updates, see [“Understanding the vGW Series Update Settings” on page 135](#).
- Support—You can use this tab to enable debug flags to generate debug messages and to collect logs to send to the Juniper Networks Support team for diagnostic purposes. You can also reboot the vGW Security VM from this tab.

**Related
Documentation**

- *Configuring Global Settings Using the vGW Series Settings Module (VMware)*
- *Installing a Secondary vGW Security VM for High Availability*
- *Understanding the vGW Security VM*
- *Understanding the vGW Security Design VM*
- *Understanding vGW Series*
- [Understanding the vGW Series Settings Module on page 3](#)

Antivirus and IDS Settings

- [Understanding and Configuring the vGW Series AntiVirus Settings on page 103](#)
- [Understanding and Configuring IDS Settings on page 104](#)
- [Understanding and Configuring IDS Signatures Settings on page 107](#)

Understanding and Configuring the vGW Series AntiVirus Settings

This topic explains the vGW AntiVirus settings and how to configure them. Before you read this topic, read *vGW AntiVirus Configuration Overview*.

The vGW Security Design VM makes configuration and installation of the vGW AntiVirus feature, including the vGW Endpoint, simple and convenient.

To configure the settings for vGW AntiVirus, you use the AV Settings section of the Settings Module. The AntiVirus Settings page allows you to enable AntiVirus, establish the frequency at which its signature database is updated, and download the vGW Endpoint.

Additionally, a status page displays detailed information, and an **About Juniper vGW Endpoint** box displays the version and build information.



NOTE: When an embedded 30 day license or a license created from the License Management System (LMS) as a Demo license is installed, you can use the vGW AntiVirus feature. However, you cannot update the signatures. That is, the signature updates part of the feature is disabled. In this case, the following message appears beneath the “Current Installed Signatures Version” line: “An appropriate license is required for signature updates”.

To update the AntiVirus signatures, a permanent license must be installed.

A vGW Endpoint runs on each protected VM. It is responsible for communicating with the vGW Security VM, monitoring file access, enforcing the AntiVirus policy, and displaying status to the user.

When AntiVirus is disabled, the vGW Security Design VM does not download new signature files, nor will it run On-Demand scans. The vGW Security VM does not load the AntiVirus module, nor does it communicate with the vGW Endpoint.

To enable and configure vGW AntiVirus settings:

1. Check the **AntiVirus Enabled** box.
2. To enable automatic update of the vGW AntiVirus signature database, in the Auto Update section:
 - a. Select **Enabled**.
 - b. Specify the interval in minutes when you want the AntiVirus signature database to be updated automatically.

This section reports the date and version of the currently installed AntiVirus signature database.

To configure the vGW Endpoint and the AntiVirus scan settings:

1. Specify the time after which the vGW Security Design VM should determine that the vGW Endpoint is disconnected.
2. Specify the number of days after which the vGW Security Design VM should consider the current AntiVirus scan outdated.

You can disable vGW AntiVirus from this pane. If you want vGW AntiVirus to remain enabled, but you do not want the AntiVirus signature database to be automatically updated, you can disable automatic updates.

To download the latest version of the vGW Endpoint, click Download. The download section identifies the version and date of the latest vGW Endpoint to allow to you better determine if you want to download it, after you initially download it.

Some administrators download the vGW Endpoint and include it in their boot scripts or software deployment packages that their organization uses. In some cases, organizations place it on a file server. For details on the vGW Endpoint, see *Understanding and Installing the vGW Endpoint*

- Related Documentation**
- *Configuring vGW Series AntiVirus On-Demand Scanning*
 - *Configuring vGW Series AntiVirus On-Access Scanning*
 - *Understanding vGW Series*

Understanding and Configuring IDS Settings

The Settings module > Security Settings > IDS Settings page allows you to configure IDS settings and IDS updates. See [Figure 29 on page 105](#).

To obtain IDS updates, you must purchase and install an IDS license.

Figure 29: IDS Settings Page

The screenshot displays the Juniper Networks configuration interface for IDS settings. The left sidebar shows a navigation tree with categories like vGW Application Settings, Security Settings, and Appliance Settings. Under Security Settings, 'IDS Settings' is selected. The main content area is split into two panes. The left pane, titled 'IDS Settings', contains 'Intrusion Detection System base settings' where 'Enable IDS' is checked. Below this are 'IDS Parameters' for HTTP and SSL ports, and a 'Global Priority Threshold' section where 'All' is selected. A 'Save' button is at the bottom right of this pane. The right pane, titled 'IDS Updates', shows the current update status with '20130331021143' for both installed and available signatures. It features a 'Check for Update' button, an 'Install' button, and radio buttons for automatic update frequency, with 'No Automatic Updates' currently selected. At the bottom, a 'Manual Update' section includes a file upload area with 'Browse...', 'Clear', and 'Upload File' buttons.

The first time that you set up IDS, you must install the IDS signatures. You use the IDS Updates pane for this purpose. First click **Check for Updates**. After the system searches for the signatures and reports that there are updates, click **Install**.

After the initial signature installation, you can use the Automatic Updates feature or you can manually insert signatures. See [Figure 30 on page 106](#).

Figure 30: IDS Updates Pane

IDS Updates

IDS signatures are updated frequently. The settings below control the behavior of the update processing.

Update Status

Currently Installed Signatures: **20130331021143**
 Signatures Available for Update: **20130428071231**
 Last Update Check: **Wed May 01 20:28:56 PDT 2013**
 Next Update Check:

Check for Update **Install**

Automatic Updates *(Hourly Check)*

☒ No Automatic Updates
☐ Download Automatically, Manually Apply Updates
☐ Download and Apply Update Automatically

Save

Manual Update

Manually upload an IDS signatures file for processing

Browse... **Clear**

Upload File

On the IDS Settings page, set the following information to configure IDS for your environment:

- IDS settings
 - Enable IDS—To turn on IDS support, select the **Enable IDS** check box.
 - IDS Parameters— Various ports can be used to pass HTTP and SSL traffic. vGW Series allows you to specify which ports should be analyzed as HTTP and which as SSL.
 - Global Priority Threshold—Specify which signatures are enabled by default based on their priority.
- IDS Updates
 - Update Status—This pane identifies the installed signatures, signatures that are available for updates, and when the last update check was performed. You can check for available signature updates and install them, if any, using this pane as you did for the initial signatures installation.
 - Automatic Updates—Automatic updates are performed hourly. You can enable automatic updates in the following ways:
 - Download Automatically and Manually Apply Updates allows you to apply downloaded signature updates yourself.

- Download and Apply Automatically allows the vGW Security Design VM to apply the updates from vGW Series servers automatically to your local environment.
- Manual Update—You can write or define custom signatures and import them into the vGW Series manually.

**Related
Documentation**

- *Configuring IDS Settings and Viewing Activity*
- [Understanding and Configuring IDS Signatures Settings on page 107](#)

Understanding and Configuring IDS Signatures Settings

This topic explains how to configure settings that control how IDS signatures are managed. You use the IDS Signatures section of the Settings module for this purpose.

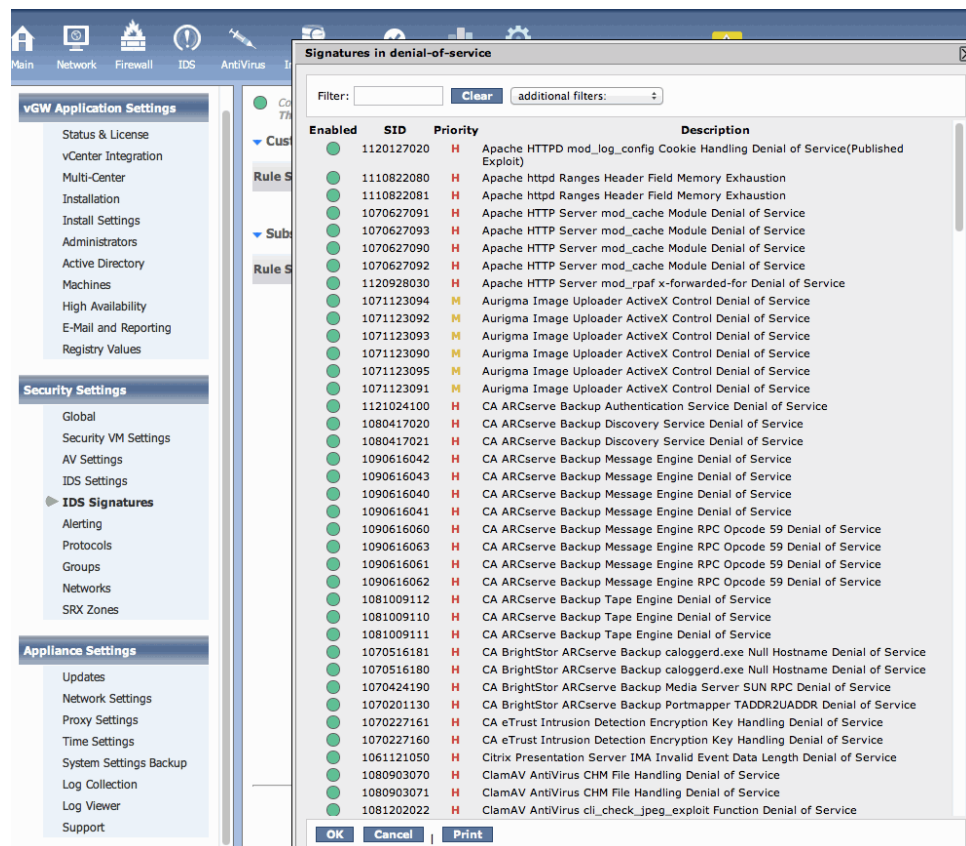
The IDS Signatures page shows the following information:

- **Custom Signatures**, if any have been uploaded. The **Custom Signatures** section does not contain entries until after you manually upload them.
- **Subscription Signatures** shows all signature groups that are part of the standard vGW Series IDS configuration.

You can activate or deactivate entire groups by selecting or deselecting the button under **Rules Selection**.

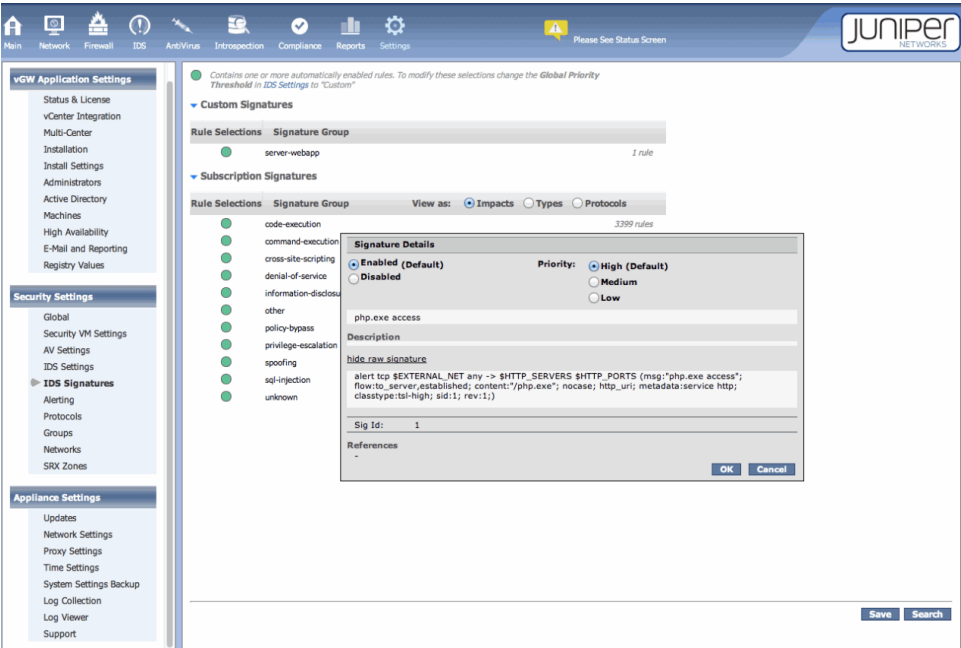
You can view the signatures that belong to a specific group. [Figure 31 on page 108](#) shows the signature rules that comprise the denial-of-service group.

Figure 31: Signatures in a Signature Group



You can also enable or disable individual signatures within a group. To do so, click the signature name in the list of signatures in the group, or the custom signature. Then select the **Enabled** button. The displayed information also provides details on the signature rule. You can change the signature priority level (high, medium, low) on the same Signature Details dialog box. See [Figure 32 on page 109](#).

Figure 32: Signature Details



NOTE: Signature sets that are loaded into the IDS engine apply to traffic that is marked, or tagged, for IDS inspection.

You can manually upload IDS custom signatures using the IDS Signatures section of the vGW Security Design VM Settings module.

Related Documentation

- *Understanding vGW Series*

CHAPTER 12

Groups

- [Understanding vGW Series Groups on page 111](#)
- [Creating vGW Series Smart Groups for VMware on page 114](#)
- [vGW Series Attributes for VMware on page 118](#)
- [About Using vGW Series Attributes for VMware on page 123](#)
- [Automatically Applying Policy Rules to VMs in Policy Groups on page 124](#)

Understanding vGW Series Groups

The Settings module **Security Settings > Groups** page lets you define groups that can contain VMs and resources. You can automate many security tasks by putting in place the proper group structure.

This topic includes the following sections:

- [Uses of Groups on page 111](#)
- [vGW Series Group Types on page 112](#)
- [Policy Groups and Monitoring Groups on page 112](#)
- [Defining the Group as a Policy Group Option with Automatic or Manual Selected on page 112](#)
- [Copying Groups on page 113](#)

Uses of Groups

Groups serve many purposes. For example, you might want to use a group for the following reasons:

- To understand how VMs belonging to the group interact on the network, but you do not want to protect their traffic.
- To use the group as source or destination term of a firewall policy rule.
- To apply policy to the VMs of a group automatically. In this case, when you create the group, you define it as a Policy Group.
- To check the compliance of VMs that belong to a group.

vGW Series Group Types

vGW Series supports the following two group types:

- *Static Groups* that allow you to define a collection of objects, such as networks, VMs, or external physical systems. A static group remains the same unless you manually change it.
- *Smart Groups* that allow for the dynamic association of VMs. To create a Smart Group, you define a set of rules, or requirements, that specify variables that characterize the group. A VM that matches one or more of a Smart Group's variables automatically becomes a member of the group.

A VM may pass in and out of Smart Groups automatically as the VM's configuration changes. Without your interaction, a VM that matches one or more of a group's variables, based on its rule requirements, is inserted into the Smart Group. If the VM's configuration is changed in such a way that it no longer meets the group's definition, the VM is automatically removed from it.

When the VM enters the group, the group's policy is applied to it. When it leaves the group, the group's policy is removed from it.

Policy Groups and Monitoring Groups

You can select the Policy Group option when you define a group to control policy association. When you select the Policy Group option, the group shows up in the Policy Groups area of the VM tree.

Groups that do not have a policy associated with them appear by default in the Monitoring Groups section of the VM tree.

The VM tree contains:

- **Policy Groups**—Contains all security policy groups, including Global, Default, and Quarantine. It also contains Illegal IPv4 Sources and Illegal IPv6 Sources groups and any policy groups that you define.
- **Monitoring Groups**—Contains all groups that were created without the Policy Group option selected, groups for monitoring the Hypervisor and Compliance state, and a group containing VMs or templates used as Gold Images by the Introspection module's Image Enforcer feature.

For details on how to enable Firewall Monitoring, see *vGW Series VMsafe Firewall + Monitoring and VMsafe Monitoring Modes*.

- **Monitored/Secured VMs**—Lists VMs monitored by the vGW Series, VMs that have a firewall protecting their network traffic, or both.

Defining the Group as a Policy Group Option with Automatic or Manual Selected

You can select the Policy Group option when you define a group to control policy association. When you select the Policy Group option, the group shows up in the Policy

Groups area of the VM tree. Groups that do not have a policy associated with them appear in the Monitoring Groups section of the VM tree.

To define a policy for the group, you use the Firewall module, select the group in the VM tree, and configure its policy rules. To install the policy, you use the Firewall Module > Apply Policy page.

Among the information that you configure for a group that you define as a Policy Group is how the policy is applied:

- Automatic—Policy changes for the group's VM members occur without your intervention. That is, you do not need to use the Firewall module's Apply Policy page to push the policy out to the VMs.
- Manual—You manually apply a policy to the VMs that belong to the group.

When you add a VM to a Smart Group or a Static Group, or a VM matches a Smart Group attribute and enters the group because of the match, the VM gets the policy rules associated with the group if the following conditions are met:

- The group is configured as a Policy Group and there is a policy containing policy rules associated with it.
- The group is configured with the Automatic option selected.

[“Automatically Applying Policy Rules to VMs in Policy Groups” on page 124](#) gives details on defining Smart Groups and Static Groups as Policy Groups with the Automatic Option to automatically “push” policies to VM members of a group.

Although a VM that enters a group—either because you added it or dynamically because it matched a Smart Group variable—gets the group's policy, this will not start to occur until after the first use.

Also, if changes are made with the vGW Series Cloud SDK, you must apply them either using the vGW Security Design VM Firewall module > Apply Policy page or using the relevant function. They do not take effect simply because the vGW Security Design VM is changed.

Copying Groups

You can use the Group page to duplicate groups.

To copy groups:

1. From the Settings module on the vGW Security Design VM, select the **Security Settings > Global**.
2. In the Groups table, click the name of the group that you want to copy.
3. Click **Copy Group**. A dialog box appears.
4. Give the new group a name.
5. If the group that you are copying is a policy group, click **Keep Policy** if you want the original group's policy to be associated with the new group.

6. For a Smart Group, you can:
 - Click **Duplicate Smart Group logic** to duplicate the rule set on the copy.
 - Click **Convert VM membership to static group** to create a static group that contains the members of the copied Smart Group.
7. Click **Save**.

The new group is added to the Groups table.



NOTE: A new group created as a copy inherits the auto push property of the original. However, because it is effectively a new group, it must be manually pushed initially.

Related Documentation • *Understanding vGW Series*

Creating vGW Series Smart Groups for VMware

This topic explains how to configure vGW Series Smart Groups. You can create groups comprised of members who meet or violate the designated match criteria defined in the Matches field of the Smart Group.

To define a Smart Group, you use the Settings module Security Settings > Groups page, and click **Add Smart Group**. The editor has two modes: Basic and Advanced. The default mode is Basic.

Suppose you want to create a compliance rule that states that all Web server VMs should have version Apache 2.x installed because of known security issues in versions 1.x. You can configure a Smart Group for a compliance rule and configure vGW Series to issue an alert when any Web server currently in production or brought online in the future has a version of Apache that is prior to 2.x.

Smart Group creation options—the parameters used to define the group—are obtained from two locations: namely, Security Design vGW attributes and vCenter attributes. Through VM Introspection, the vGW Security Design VM can discover items such as which applications are installed on a VM, while VMware's vCenter identifies attributes such as the port group to which the virtual network interface is connected. There are numerous attributes each classified into “vf” (vGW-based) and “vi” (vCenter-based) categories as described in the topic [“vGW Series Attributes for VMware” on page 118](#).

The following values are returned for the Type field.

- Boolean: True or False
- Integer: Numeric value
- String: Free-form text string

- Multi String: Multiple string values concatenated together with separators such as commas, semicolons, or slashes
- Multi Value: List of available choices

In Basic mode you can select one or more attributes and assign an **All** or **Any** constraint. You add rules by clicking the + sign.

Figure 33 on page 115 shows a group called WebServers that is created when the VMware vCenter name (vi.name) contains www and the application named Apache is installed on the VM. Both conditions must exist for a VM to be included in this group. The information that defines this Smart Group is obtained through VI Introspection and is stored in vf.application.

Figure 33: Creating a Smart Group Using Basic Mode

Add Group

Name:

Advanced

Matches: ☒ All ☐ Any

vi.name	Contains	www	-	+
vf.application	Contains	apache	-	+

Group Policy Attributes:

☒ Policy Group

Priority:

Apply Policy: ☐ Automatic ☒ Manual

Test Save Cancel

To define a Smart Group using basic mode:

1. Select **Setting > Security Settings > Groups**.
2. To create a new Smart Group:
 - a. Click **Add Group**.
 - b. On the displayed pane, click **Add a Smart Group**.

If you do not know the meaning of an attribute or the values that it can take, click ? at the end of the row. The pop-up message box that appears describes the attribute. It gives its data type, and it identifies possible values.

3. Give the Smart Group a short, descriptive name. The name is displayed in the Groups table.
4. For Matches, select **All** if the VM must meet all criteria defined in the field below or **Any** if the VM can meet any of the criteria defined in the field below.
5. For each row, select the following information:
 - An attribute.

- A comparator. For example, you can require that a VM must meet the attribute specification to be associated with the group, or you can define a rule that excludes VMs that meet the criteria.
 - A value.
6. Select the **Policy Group** check box if you want the Smart Group to belong to a policy group.

When you select Policy Group:

- The Smart Group is added to the Policy Groups area in the VM tree.

You can now configure a firewall policy for the Smart Group on its Group Policy page. You use the Firewall module in conjunction with the VM tree to display the Smart Group's policy page.

- Specify a priority level and a precedence level:
 - You can select high, medium (default), or low for the priority level.
 - You can use **Precedence** within **Level** to define the precedence for Smart Groups that are created with the same priority level.



NOTE: A VM can belong to more than one Smart Group. In this case, the policy rules of all Smart Groups that the VM is a member of are applied to the VM. How the rules are applied also depends on the precedence and priority settings.

It can happen that more than one Smart Group is defined with the same priority level and the same precedence within that level. In this case, Smart Group rules are applied to the VM in the order in which the Smart Groups were created.

7. Test the configuration before you save the Smart Group definition. Click **Test** to verify that the group contains the VMs that you intended it to include.

In addition to creating a Smart Group by adding rows to the rules table using Basic mode, the editor's Advanced mode allows you to write regular expressions to construct more complicated scenarios. [Figure 34 on page 117](#) shows how to define the simple WebServers example in Advanced mode using a regular expression.

Figure 34: The Smart Group Editor in Advanced Mode Using Regular Expressions

Add Group

Name:

Basic

Selection query:

Group Policy Attributes:

☒ Policy Group

Priority:

Apply Policy: ☐ Automatic ☒ Manual

The selection query allows you to define expressions based on a simple set of operators. You can write an expression in the context of each VM, getting its attributes, and if the expression evaluates as True, the VM becomes part of the group. [Table 5 on page 117](#) covers the various Smart Group attribute types and operators.

Table 5: Operators for Creating Smart Groups Using Regular Expression

Attribute Type	Supported Operators
String	<p>The most common attribute type.</p> <p>Contains (~), Not-Contains (!~), Equals (=), Not-Equals (!=), Matches RegExp (=~).</p> <p>Full wildcard support such as name = "finance-*" is recognized.</p>
Numerical	Equals (=), Greater than (>), Not-Equals (!=), Less-Than (<), In (in), Not in (not_in).
IP	Equals (=), In (in), Not in (not_in).
Boolean	Equals (=), Not-Equals (!=) Return value is either true or false. For example, vf.secured = false or vf.secured != true.
Multi	Contains (~), Not-Contains (!~), Equals (=), Not-Equals (!=), Matches RegExp (=~).
Group	Contains (~), Not-Contains (!~), Equals (=), Not-Equals (!=), Matches RegExp (=~).

You can also create wildcard matches if you match on a full string. For example:

- `.*WWW.*` - Match VMs with WWW anywhere in the name"
- `^Corp.*` - Matches VMs starting with Corp
- `.*1$` - Matches VMs ending with "1".

- `.*Tier-[1-3].*` - Match VMs with Tier-1/2/3"
- `^[ABC].*` - Match VMs starting with A, B, or C.

**Related
Documentation**

- [About Using vGW Series Attributes for VMware on page 123](#)
- [vGW Series Attributes for VMware on page 118](#)
- [Understanding vGW Series Groups on page 111](#)
- [Understanding vGW Series](#)

vGW Series Attributes for VMware

Table 6 on page 118 identifies the attributes that you can use in defining Smart Groups.

Table 6: Smart Group Attributes

Attribute name	Data Type	Description
vcd.tag	String	vCloud Director Organization and metadata attributes.
vf.antivirus.database.version	String Value	What version of AV database version is this VM using? (What's installed on the central AV database it is connected to)?
vf.antivirus.endpoint.connected	Boolean Value	Is this VM properly connected to central AV scan engine?
vf.antivirus.endpoint.enabled	Boolean Value	Does this VM have an operational AV agent installed?
vf.antivirus.endpoint.version	String Value	Version of endpoint installed on the VM.
vf.antivirus.engine.version	String Value	What version of the AV engine is this VM is using? (What is installed on the central VM database it is connected to?)
vf.antivirus.onaccess.enabled	Boolean Value	Does this VM have on-access AV scanning enabled?
vf.antivirus.quarantine.enabled	Boolean Value	Is this VM configured to quarantine virus files?
vf.app_count_bad	Integer	Number of applications on a VM that are classified as bad.
vf.app_count_known	Integer	Number of applications on a VM that are classified as known.
vf.app_count_unclassified	Integer	Number of applications on a VM that are unclassified.

Table 6: Smart Group Attributes (*continued*)

Attribute name	Data Type	Description
vf.app_count_unknown	Integer	Number of applications on a VM that are classified as unknown.
vf.app.gi.compliant	String Value	Is this VM in compliance with the selected Gold Image?
vf.app.is.gold.image	Boolean Value	Is this VM defined as a master image for Image Enforcer comparisons?
vf.app.matches.gold.image	Boolean Value	Is this VM compliant with its configured Gold Image?
vf.app.registry	String Value	Registry value from s registry as determined by Introspection of VM.
vf.application	String Value	An application installed on a VM.
vf.description	String	The text string description of the VM, as defined in the vGW Security Design Settings module Machines section.
vf.firewall	String	Is this VM a vGW Security VM?
vf.group	Multi String	Comma-separated string of all vGW groups to which a VM belongs.
vf.has_installed_group_policy	Boolean	Does the VM have a non-default group policy installed?
vf.has_installed_policy	Boolean	Does the VM have an installed security policy?
vf.hotfix	Multi String	Hotfix installed on a VM.
vf.monitored	Boolean	Is the VM currently being monitored by the vGW Security Design VM?
vf.name	String	Name as defined in the vGW Security Design VM.
vf.os	String	The operating system installed on the VM.
vf.quarantined	Boolean Value	Is this VM in a quarantined state, and thus in the Quarantine Policy group?
vf.secured	Boolean	Is a VM currently secured by the vGW Security Design VM?
vf.secured_active	Boolean	Is the VM actively protected by vGW?

Table 6: Smart Group Attributes (*continued*)

Attribute name	Data Type	Description
vf.tag	String	Tags associated with this VM that are semicolon separated.
vf.type	Enumeration	The machine object type.
vf.virus.infected	Boolean Value	Has a virus been detected on this VM by the vGW antivirus engine?
vi.attribute	String Value	The attribute values that are defined in the annotation box in VI.
vi.cluster	String	Cluster containing a VM.
vi.datacenter	String	Data Center in vCenter where a VM is housed.
vi.deleted	Boolean Value	Has this VM been deleted?
vi.excfg.copy.disable	Boolean Value	Is the copy and paste to remote console feature disabled for this VM?
vi.excfg.deviceconnectable.disable	Boolean Value	Is this VM configured to allow devices to be connected?
vi.excfg.deviceedit.disable	Boolean Value	Is this VM configured to allow devices to be connected and removed?
vi.excfg.diskshrink.disable	Boolean Value	Is this VM configured to prevent virtual disk shrinking?
vi.excfg.diskwiper.disable	Boolean Value	Is this VM configured to prevent virtual disk shrinking?
vi.excfg.dragndrop.disable	Boolean Value	Is the copy and paste to remote console feature disabled for this VM?
vi.excfg.hostinfo.disable	Boolean Value	Is access to host performance information available to this VM?
vi.excfg.log.disable	Boolean Value	Is the VM log file size limited for this VM?
vi.excfg.log.keep.old	Numeric Value	Is the number of stored log files limited for this VM?
vi.excfg.log.rotatesize	Numeric Value	Is the VM log file size limited for this VM?
vi.excfg.paste.disable	Boolean Value	Is the copy and paste to remote console feature disabled for this VM?

Table 6: Smart Group Attributes (*continued*)

Attribute name	Data Type	Description
vi.excfg.remotedisplay.max	Numeric Value	How many remote consoles are available for this VM? VMware Hardening guideline recommends limiting to one.
vi.excfg.remoteop.disable	Boolean Value	Are remote operations disabled for this guest?
vi.excfg.setguiopts.disable	Boolean Value	Is the copy and paste to remote console feature disabled for this VM?
vi.excfg.vmxfilesize.limit	Numeric Value	Is the VMX file size limited (to limit the informational messages from VM to VMX file) ?
vi.folder	Multi-String	The folder containing a VM in vCenter.
vi.host	String	ESX/ESXi hosting a VM.
vi.host.console.ids	Boolean Value	Is vGW IDS inspection enabled for this hypervisor's service console?
vi.host.console.monitor	Boolean Value	Is vGW network monitoring enabled for this hypervisor's service console?
vi.host.lockdown	Boolean Value	Is lockdown mode enabled for this hypervisor host?
vi.host.ntp.enabled	Boolean Value	Is Network Time Protocol (NTP) configured and enabled for this hypervisor?
vi.host.techsupportmode.disable	Boolean Value	Is tech support mode enabled for this hypervisor?
vi.host.vmkernel.isolated.vlan	Boolean Value	Is the vmkernel management network on this hypervisor on an isolated VLAN?
vi.host.vmkernel.isolated.vswitch	Boolean Value	Is the vmkernel management network on this hypervisor on an isolated vSwitch?
vi.indep.nonpersist.disk.ct	Numeric Value	The number of virtual disks used by this VM that are configured as Independent nonpersistent and thus cannot be introspection scanned.
vi.ipv4	IPv4 (multi value)	The IP addresses as known on a VM.

Table 6: Smart Group Attributes (*continued*)

Attribute name	Data Type	Description
vi.ipv6	IPv6 (multi value)	<p>The IP addresses as known on a VM. They can be coded as single addresses or an address range.</p> <p>Example Addresses:</p> <ul style="list-style-type: none"> • 2001:0db8:85a3:0000:0000:8a2e:0370:7334 • fe80::202:b3ff:fe1e:8329
vi.memory_inspection	Boolean	Are VMsafe memory and CPU API enabled for this VM?
vi.name	String	Name of this VM as defined in vCenter.
vi.notes	String	Annotation free text notes attached to the VM in vCenter.
vi.os	String Value	Operating system defined for the VM in vCenter.
vi.pg.security.forgedtransmits	Boolean Value	Is VM connected to a port group that allows forged MAC addresses (MACs other than defined in the VMX)?
vi.pg.security.macchanges	Boolean Value	Is VM connected to a port group that allows reception of unknown MAC addresses (MACs other than defined in the VMX)?
vi.pg.security.promiscuous	Boolean Value	Is VM connected to a promiscuous port group?
vi.portgroup	String Value	Port groups on the virtual switch this VM is actively connected to. Port Groups for disconnected vNICs will not be included. (For a running/suspended VM, this will be the port groups actually connected. For a stopped VM, this value is the port groups that are connected at poweron.)
vi.portgroup.all	String Value	Port groups on the virtual switch this VM is connected to. This list includes port groups even if the vNIC is disconnected. (For a running/suspended VM, this will be the port groups actually connected. For a stopped VM, this value is the port groups that are connected at poweron.)
vi.powerstate	Enumeration	What is the current power state of this VM?
vi.pvlan	Numeric Value	Private VLAN values for connected port groups.
vi.pvlan.all	Numeric Value	List of all private VLANs in use by this VM, includes vNICs in both connected and disconnected states.

Table 6: Smart Group Attributes (*continued*)

Attribute name	Data Type	Description
vi.os	String	Operating system defined for the VM in vCenter
vi.resourcepool	String	Resource pool VM is a member of vCenter.
vi.snapshots.count	Numeric Value	How many snapshots exist for this VM?
vi.vapp	Multi String	vApp group VM is a member of vCenter.
vi.vlan	Multi-value integer	VLANs of connected port groups.
vi.vlan.all	Multi-value integer	VLANs of all interfaces.
vi.vmci_enabled	Boolean	Is VMCI (shared memory communications) enabled for this VM?
vi.vmsafe_configured	Boolean	Is VMSafe firewall security enabled for this VM?
vi.vmsafe_dvfilter	Multi String	The dvfilters protecting this VM.
vi.vmsafe.initfailmode	Enumeration	If VMSafe is unable to initialize, what is the network connectivity choice for this VM?
vi.vmwaretools.running	Boolean	Is VMware Tools running on this VM?
vi.vmwaretools.uptodate	Boolean	Is the version of VMware Tools installed on this VM current?
vi.vnic.count	Numeric Value	Number of connected vNICs.
vi.vswitch	Multi String	vSwitch VM is connected to.

Related •
Documentation

About Using vGW Series Attributes for VMware

vGW Series continuously analyzes both its own and the VMware objects databases in relation to the Smart Group rules that you configure to determine if a VM should belong to a Smart Group or not. The rules that you configure to define a Smart Group are obtained from these locations:

- vGW Series Smart Group attributes. These attributes are categorized and labeled with the prefix *vf*.
- VMware vCenter attributes. These attributes are labeled with the prefix *vi*. VMware's vCenter identifies attributes such as the port group to which the virtual network interface is connected.

- VMware vCloud Director attributes. These attributes are labeled with the prefix *vcd*. The vGW Security Design VM obtains metadata associated with a VM from the vCloud Metadata tab page for the VM.

You can associate Smart Groups with a firewall policy. Policy association is controlled by the Policy Group option that you can select when you define the Smart Group.

Using Smart Groups, you can streamline policy application to ensure security efficiently throughout your virtual infrastructure. Firewall policies are applied to VMs instantly without your intervention when a VM becomes a member of a Smart Group. Consider these two cases in which firewall policies are automatically applied to VMs:

- Suppose that you associate the virtual network interface of a VM with the corporate production network. As a consequence of the configuration change, the VM meets a Smart Group's rule that specifies the *vi.portgroup* attribute and matches the configuration. In this case the VM becomes a member of the Smart Group, and the Smart Group's firewall policies are applied to it.
- Suppose that you define a Smart Group that checks for VMs connected to a particular VMware resource pool that is specified in a rule that uses the *vi.resourcepool* attribute. When you add a VM to this resource pool, the VM is added to the Smart Group and the Smart Group's firewall policies are applied to it.

**Related
Documentation**

- [Understanding vGW Series Groups on page 111](#)
- [Understanding vGW Series](#)
- [Creating vGW Series Smart Groups for VMware on page 114](#)
- [vGW Series Attributes for VMware on page 118](#)

Automatically Applying Policy Rules to VMs in Policy Groups

vGW Series allows you to create Static Groups or Smart Groups that are defined as Policy Groups and then associate policy rules with them. If you select the Automatic option for the group when you configure it, when a VM joins the group, the policy rules associated with the group are automatically applied to the VM.

Configuring a group as a Policy Group whose rules are applied automatically to its VM members entails:

- Creating either a Static Group or a Smart Group and selecting the Policy Group and Automatic options. Use the Settings > Security Settings > Groups page.

The Groups page allows you to define a Static Group or a Smart Group and attributes for it. You can specify that the group is a Policy Group and you can select Automatic for it. If you select Automatic, rules defined for the policy group are applied automatically to VMs that join the group. You can add VMs to a policy group (Static Group) or they join it dynamically because they match one or more of the group's configured variables (Smart Group). In either case, when the VM joins the group, it gets the group policy rules.

- Securing the group with a firewall policy. Use the Firewall module to create the policy rules for the group and apply (install) the policy rules.

When you add a VM to a Smart Group or a Static Group or a VM matches a Smart Group attribute and enters the group because of the match, the VM gets the policy rules associated with the group if the following conditions are met:

- The group is configured as a Policy Group and there is a policy containing policy rules associated with it.
- The group is configured with the Automatic option selected.

After you create a policy group, it is added to the Firewall > Apply Policy table, ready to be applied to the group. The policy group must be applied once before it can be used for auto-push. Note that auto push will apply the policy to a VM automatically only when the VM enters or exits the group based on matching.

This example shows how to create a group that automatically pushes its policy to VMs that belong to the group or join it dynamically. It creates a Smart Group called HighPriorResGrp, and it configures it as a Policy Group with the Automatic option selected.

1. On the Settings > Security Settings > Groups page, configure a Smart group called HighPriorResGrp that watches for any VMs connected to a particular VMware resource pool (called high-prior-res) obtained through vi.resourcepool.

Smart Groups specify attributes that a VM must match to join the group. For details on Smart Groups, see *Understanding vGW Series Smart Groups*.

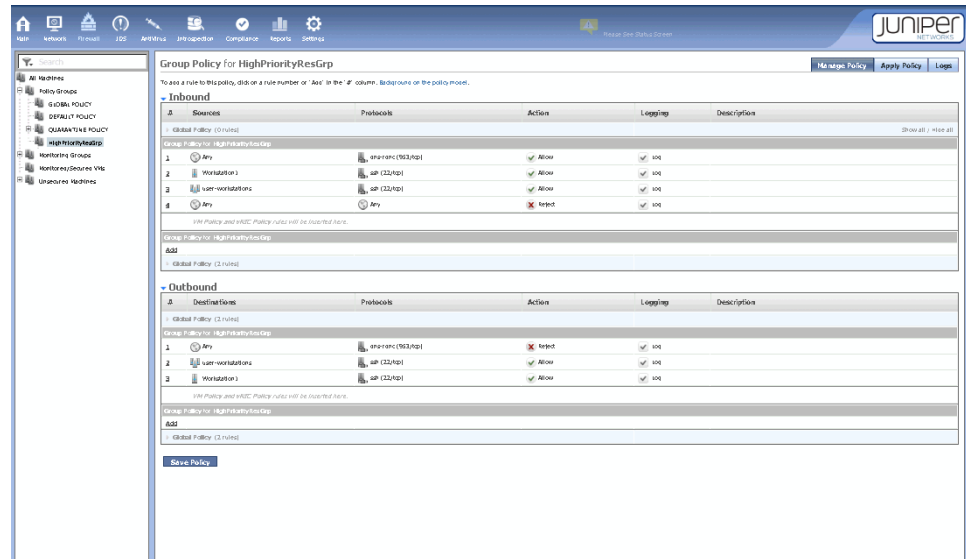
When a VM joins the Policy Group, the group's rules are instantly installed on that VM without requiring any intervention on your part. [Figure 35 on page 125](#) shows the Smart Group configuration. Notice that **Policy Group** and **Automatic** are selected for the Group Attributes.

Figure 35: Configuring a Smart Group As a Policy Group

2. Configure policy rules for the HighPriorityResGrp Smart Group.

When you create a group and define it as a Policy Group, vGW Series places it in under Policy Groups in the VM Tree. You can click on the group name to display the Firewall > Manage Policy tab that allows you to configure group rules. See [Figure 36 on page 126](#).

Figure 36: Configuring Policy Rules for a Smart Group with Policy Group Enabled



Related Documentation

- [Understanding vGW Series](#)
- [Understanding the vGW Security VM](#)
- [Understanding the vGW Series Application Settings on page 7](#)
- [Understanding Policy per vNIC and Smart Groups for VMware Environments on page 55](#)

CHAPTER 13

Alerts

- [Understanding the vGW Series Security Alert Settings on page 127](#)

Understanding the vGW Series Security Alert Settings

This topic covers the events sent by e-mail and SNMP and how to configure Alert settings for e-mail and SNMP traps.

It includes the following sections:

- [Event Types on page 127](#)
- [E-mail Alert Settings on page 127](#)
- [SNMP Trap Settings on page 128](#)
- [AutoConfig and Multicast Alerts on page 128](#)

Event Types

vGW Series sends security alerts (Main→Events and Alerts→Security Alerts) by e-mail and SNMP. Security Alerts have high, medium, and low (H/M/L) priorities. By default, alerts of all priorities are sent by SNMP and e-mail. However, you can use the `center.conf` parameter `center.alert.notification.priority` to change this configuration. By default, it is set to 3 (low). Alerts with a priority that is equal to or lower than the configured value are sent.

E-mail Alert Settings

You enable e-mail alerts by providing the mail relay server IP address and the source and destination e-mail addresses. vGW Series supports both IPv4 and IPv6 addresses. The aggregation time is the gap between successive notifications.

You do not need to configure multiple e-mail recipients. However, you can create four custom e-mail alert tags that point to different e-mail aliases or individual e-mail accounts, or a combination of the two. You can specify these custom tags in the security policy editor.

To send both an e-mail alert and an SNMP trap on a single rule, you use the standard alert icon. In this case, only the e-mail addresses listed in the **Recipients Addresses** are used. That is, you can not use custom tags when you send e-mail and SNMP alerts.

SNMP Trap Settings

An Simple Network Management Protocol (SNMP) trap is an asynchronous notification from agent to manager. It includes the current sysUpTime, and OID identifying the type of trap, and optional variable bindings. SNMP traps can be set via Version 1 or Version 2. You must enter the SNMP server address and community string. Optionally, you can set the aggregation time again (the delay between successive events).

To configure SNMP using the Settings module Alerting > SNMP Trap Settings pane:

- Select the **Enable** check box if you want to send SNMP traps on alerts.
- Select the SNMP version to use. By default Version 1 (SNMPv1) is selected.
- Specify the SNMP monitor address.
- Specify the SNMP community string.
- Specify the aggregation time in seconds.
- Click **Save**.

AutoConfig and Multicast Alerts

By default, the vGW Series is configured to alert when autoconfig addresses are discovered (Settings page -> Security Settings -> Alerting). No alert is automatically sent when Multicast is seen (though this can be enabled).

- **Autoconfig addresses**—When a machine does not have an IP address configured or it can not acquire a DHCP lease, it defaults to using an autoconfig address in the 169.254.*.* range. Often this setting represents a configuration problem or an issue with the DHCP service.
- **Multicast**—Many hosts use multicast packets to advertise their presence on the network. They also send broadcast information about the services that they offer, and configuration data. This information is often not needed, so it can be undesirable for servers to provide it. In addition, there are security issues related to advertising the services a machine has available.

Related Documentation

- *Understanding vGW Series*

CHAPTER 14

SRX Series Devices

- [Understanding the vGW Series SRX Zones Settings on page 129](#)

Understanding the vGW Series SRX Zones Settings

You can use the SRX Zones section of the Settings module of the vGW Security Design VM to create interoperability with physical SRX Series devices. For details, see *vGW Series and SRX Series Security Zones*. vGW Series integration with SRX Series zones allows it to obtain zone information from an SRX Series device and populate the vGW Security Design VM with that information. vGW Series can also put VM information into SRX Series address books that allows you to know which VMs are mapped to each zone.

Related Documentation

- *Understanding vGW Series*

CHAPTER 15

Networks and Protocols

- [Understanding the Settings Module Networks Settings on page 131](#)
- [Understanding vGW Series Protocols Support on page 131](#)

Understanding the Settings Module Networks Settings

You can use the Settings module **Security Settings > Networks** page to define network objects for use in vGW Series firewall policies. You can define a network by IP Range or Subnet Mask. vGW Series supports IPv4 and IPv6 environments, and, as such, network ranges in both address spaces.

Related Documentation

- [Understanding vGW Series](#)
- [Understanding vGW Series IPv6 Support](#)
- [Configuring the vGW Series Policy per vNIC Feature on page 50](#)

Understanding vGW Series Protocols Support

By default, the protocols table shows all IANA registered protocols. You can add to this table custom protocols or other application protocols that are not IANA registered. Protocols that you add are shown by name in network reports instead of being displayed by port or protocol.

You can also define your own non-TCP and non-UDP protocols, such as GRE and IPsec protocols. You can define protocol ranges such as Custom App /TCP/8000-8005.

The Protocols table displays the name of a protocol, its type, such as TCP, UDP, ICMPv6 and the number of the port used for it.

You can combine a number of protocols into a Protocol Group so it can be used in Firewall Policy creation (for example, for Global, Group, or Individual VMs). To do so, click **Add**, enter a name for the group, and select the appropriate protocols, and then click **Save**.

The protocols table includes individual ICMPv6 protocols and also a default ICMPv6 protocol group that allows inbound traffic for a group of ICMPv6 protocols. vGW Series allows all inbound and outbound Internet Control Message Protocol version 6 (ICMPv6) traffic. ICMPv6 is integral to IPv6 and fundamental to the proper functioning of IPv6 networks. For details on how the vGW Series firewall handles ICMPv6 protocols and the

default protocol group for ICMPv6 protocols, see *Understanding How vGW Series Handles ICMPv6 Protocol Traffic*.

- icmp6-all: all possible types
- a new transport protocol type was added for ICMPv6 (icmpv6). For it, you must specify the type of the protocol (number) in the Type: box.
- other new IPv6 protocols:
- dhcp6-client
- dhcp6-server
- ripng
- route-ipv6
- frag-ipv6
- nonxt-ipv6
- opts-ipv6
-

**Related
Documentation**

- *Understanding vGW Series*

PART 4

Appliance Settings

- [Updates on page 135](#)
- [Networks and Proxies on page 139](#)
- [Time on page 143](#)
- [Backup and Restore on page 145](#)
- [Logs on page 151](#)
- [Support on page 155](#)

CHAPTER 16

Updates

- [Understanding the vGW Series Update Settings on page 135](#)
- [Updating the vGW Security Design VM on page 135](#)
- [Updating vGW Security VMs in Batch Mode on page 137](#)

Understanding the vGW Series Update Settings

The vGW Security Design VM has a built-in mechanism for updating and upgrading any vGW Series component with new security protections, bug fixes, and other enhancements. You use the Settings > Appliances Settings > Updates page to update and upgrade the vGW Security Design VM and the vGW Security VMs. The Updates page includes these parts:

- The Security Design vGW Update pane that shows the last time that the vGW Security Design VM checked for and installed an update. To manually check for updates, click **Check for Updates**.
- The Update Preferences pane enables the vGW Security Design VM to automatically check Juniper Networks Internet update servers for the latest software.
- The Security VM Batch Updates pane lets you update multiple vGW Security VMs immediately or schedule them to be updated. To manually check for updates, click **Check for Updates**

Related Documentation

- [Updating the vGW Security Design VM on page 135](#)
- [Updating Individual vGW Security VMs](#)
- [Updating vGW Security VMs in Batch Mode on page 137](#)
- [Understanding vGW Series](#)
- [Understanding the vGW Series Settings Module on page 3](#)

Updating the vGW Security Design VM

This topic covers how to update the vGW Security Design VM online and offline manually.

This procedure explains how to update the vGW Security Design VM online. In this case, the vGW Security Design VM must be able to connect to the Juniper Networks update servers (HTTPS - TCP 443).

To update the vGW Security Design VM manually:

1. Ensure that a proper entitlement key is installed on the vGW Security Design VM.

If it is not already installed, insert the entitlement key in the vGW Application Settings -> Status & License section of the Settings module. This section also allows you to see the update status of the vGW Security Design VM

- a. In the Product Licensing section, click **Manage Licenses**.

A table showing the installed licenses is displayed.

This section also allows you to see the update status of the vGW Security Design VM.

Without an entitlement key, you cannot activate and install an update. You obtain the entitlement key when you purchase the product and software subscription contract.

2. Navigate to Settings > Appliance Settings > Updates.

- a. Click **Check for Updates** to query the Juniper Networks update servers.

The update server checks to determine if the component requires an update.

- b. If an update exists, click **Update Now** to apply the changes.

vGW Series downloads the required updates from the Juniper Networks server. In some cases, the vGW Security Design VM will need to be rebooted.

Updating the vGW Security Design VM Offline

This procedure explains how to update the vGW Security Design VM offline, that is, without using Internet access. It uses an ISO image connected to the vGW Security Design VM for this purpose.



NOTE: Before you can update the vGW Security Design VM offline, you must obtain the update ISO from the Juniper Networks Support team and mount it on the vGW Security Design VM.

Before you can update the vGW Security Design VM offline, you must obtain the update ISO from the Juniper Networks Support team and mount it on the vGW Security Design VM.

To perform a manual update offline:

1. In the Settings module Appliance Settings > Updates > section, click **Advanced**.
2. Obtain the update ISO from the Juniper Networks support team, and mount it on the vGW Security Design VM.
3. Select the **Offline Update** check box.

4. Click **Connect Update Media**.
5. To check for updates first, click **Check for Updates**.
6. Click **Update Now**.

Updating the vGW Security Design VM Offline

This procedure explains how to update the vGW Security Design VM offline. Before you can update the vGW Security Design VM offline, you must obtain the update ISO from Juniper Networks Support and mount it on the vGW Security Design VM.

To perform a manual update offline:

1. In the Settings module Appliance Settings > Updates > section, click **Advanced**.
2. Select the **Offline Update** check box.
3. Click **Connect Update Media**.

In the Appliance Settings > Updates > Security Design vGW Update section, click **Check for Updates**.

4. To check for updates first, click **Check for Updates**.
5. Click **Update Now**.

Related Documentation

- [Understanding the vGW Series Update Settings on page 135](#)
- [Updating Individual vGW Security VMs](#)
- [Updating vGW Security VMs in Batch Mode on page 137](#)
- [Understanding vGW Series](#)
- [Understanding the vGW Series Settings Module on page 3](#)

Updating vGW Security VMs in Batch Mode

This topic explains how to update vGW Security VMs as a group in batch mode.

When you update vGW Security VMs in batch mode, you can run the updates immediately or schedule them to run later.

To set up the system to update vGW Security VMs in batch mode:

1. Navigate to the Settings module Appliance Settings > Updates page.
2. In the Security VM Batch Updates pane, enter the **Custom Product** version.
3. Select the check boxes for the vGW Security VMs that you want to update. You can select all of them at once.
4. Specify whether you want the updates to run when the ESX/ESXi host is in Maintenance mode. Select:
 - **Always**, in which case logs are not lost.

- **As needed** for kernel driver updates only.
 - **Never.**
5. Using the **Start Time** option buttons, specify when to run the batch update process.
- To begin the batch update process immediately, select **Now**. Click **Update**.
 - To schedule the batch update, select **Later**.
 - a. Enter a start date and a start time.
 - b. Optionally, enter an end time.

If you specify an end time, vGW Series completes any update that is in progress when the end time is reached. However, it will not begin any new vGW Security VM updates.

- c. Optionally, enter an e-mail account to which an update status message is sent when the update either completes or is interrupted.

If you specify an e-mail address for Status email, a message reporting on the vGW Security VMs that were updated and those that are pending is sent to the recipient.

**Related
Documentation**

- [Understanding the vGW Series Update Settings on page 135](#)
- [Updating the vGW Security Design VM on page 135](#)
- [Updating Individual vGW Security VMs](#)
- [Understanding vGW Series](#)
- [Understanding the vGW Series Settings Module on page 3](#)

Networks and Proxies

- [Configuring the vGW Series Network Settings on page 139](#)
- [Configuring vGW Series Proxy Settings on page 142](#)

Configuring the vGW Series Network Settings

This topic covers the Settings module Appliance Settings > Network Settings page which allows you to change the name of the vGW Security Design VM and configure network information for it. It explains how to configure the vGW Security Design VM for dual stack.

You use the Network Settings page to configure the following information:

- **Host Name:** Change the name of the vGW Security Design VM.

You can specify a different name for the management center which is called vGW Security Design VM by default.



WARNING: Do not change the vGW Security Design VM name during any configuration that involves its interaction with VMware vCenter. This includes installing, un-installing, or updating the vGW Security Design VM.

- **DNS Settings:** Use either of the following methods to specify how vGW Security Design VM obtains IP addresses and other information from Domain Name System (DNS):
 - Select **Use DHCP to Get DNS**, if you want to use Dynamic Host Configuration Protocol (DHCP) to get the IP address of a DNS server dynamically.
 - **Primary DNS Server:** To use a particular DNS server, de-select **Use DHCP to Get DNS**. Then specify the IP address of the primary DNS server, and optionally, a secondary one.

You can also specify a search domain to use for resolving system names and addresses within vGW Security Design VM reports. To specify more than one search domain, use spaces to separate the specifications.

- **Search Domain:** Specify a search domain to use for resolving system names and addresses within vGW Security Design VM reports. To specify more than one search domain, use spaces to separate the domains.

- **Interface 1:** Configure this virtual NIC (vNIC) to be used for dual stack support or to be dedicated to *either* IPv4 or IPv6. When dual stack is used, this configuration specifies both IPv4 address and IPv6 address information.

This interface is used for management communication with vGW Security VMs. It must be reachable by the management vNICs of vGW Security VMs.

To *not* use dual stack for the vGW Security Design VM, disable either IPv6 or IPv4.

- To use only IPv4 for vGW Security Design VM management communication with the vGW Security VMs, disable IPv6. In the **IPv6:** box, select **Disabled** from the list.
- To use only IPv6 for vGW Security Design VM management communication with vGW Security VMs, disable IPv4. In the **IPv4:** box, select **Disabled** from the list.

To configure dual stack for the vGW Security Design VM interface (vNIC) for management communication with vGW Security VMs:

- **IPv4:**

For IPv4, from the displayed list, select the method to use to assign an IPv4 address to the vNIC:

- **DHCP**

Use a DHCP server to assign dynamically an IPv4 address to the vNIC.

- **Static IP**

Specify a static IP address and its network mask routing prefix, and the default gateway to assign to the vNIC.

- **IPv6:**

- **DHCPv6**

Use a DHCPv6 server to obtain the IPv6 address for this vNIC.

As RFC 3315 states "The Dynamic Host Configuration Protocol for IPv6 (DHCP) enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to "IPv6 Stateless Address Autoconfiguration" (RFC 2462)

- **Autoconfiguration**

Use stateless address autoconfiguration to obtain the IPv6 address for this vNIC. IPv6 stateless address autoconfiguration allows network devices attached to an IPv6 network to automatically acquire IP addresses and connect to the Internet without intermediate interaction with a DHCPv6 server.

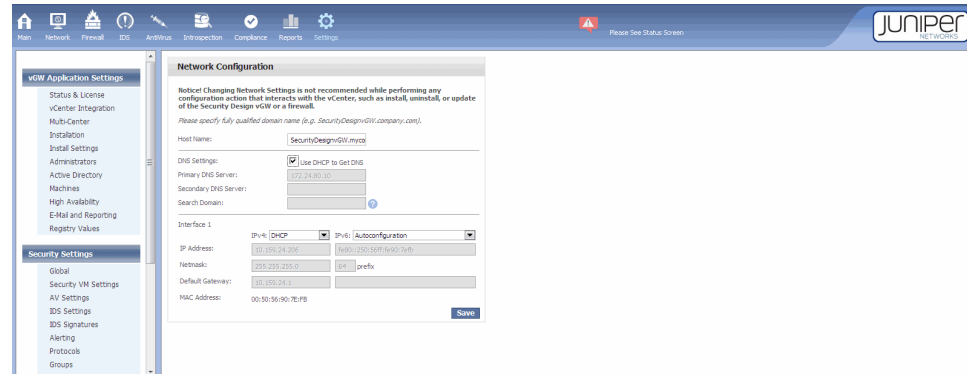
Refer to RFC 2462, "IPv6 Stateless Address Autoconfiguration" for details.

- **Static IP**

Specify a static IP address for the vNIC including the IPv6 address prefix (the initial bits of the address that denote the network address, akin to a netmask), and the default gateway to use for it.

Figure 37 on page 141 shows the Network Configuration page with vGW Security Design VM configured for dual stack support. Interface 1 is configured to use DHCP to obtain its IPv4 address and stateless address autoconfiguration to obtain its IPv6 address.

Figure 37: Settings Module Network Settings Configuration for Dual Stack Support



The vGW Security Design VM cannot communicate with any vGW Security VMs or the standby vGW Security Design VM if the types of their IP addresses differ from the type of IP address assigned to the vGW Security Design VM.

Communication problems between the vGW Security Design VM and vGW Security VMs should not exist in an environment in which the vGW Security Design VM is configured for dual stack and some vGW Security Design VMs have IPv4 addresses while others have IPv6 addresses. The environment might also include a standby, or secondary, vGW Security Design VM used for high availability with either type of IP address and that, too, would pose no problems with a dual stack vGW Security Design VM.

However, if you change the configuration for the vGW Security Design VM from dual stack to single with only one IP address assigned to its interface 1 vNIC—for example, IPv6—communication problems with any vGW Security VMs with IPv4 addresses will occur. That holds true for the standby vGW Security Design VM also if it had an IPv4 address bound to it.

In circumstances where the IP address types differ, vGW Series presents the following error messages:

- When your environment includes a vGW Security VM—called SVM for example—that has only an IPv6 address bound to it, if you attempt to change the vGW Security Design VM from dual stack to single with only an IPv4 address bound to it, vGW Series displays the following message
 “The interface for management communications must have an IPv6 configuration, because Security VM SVM1 has only IPv6 interface.”
- When your environment includes a vGW Security VM—called SVM for example—that has only an IPv4 address bound to it, if you attempt to change the vGW Security Design VM from dual stack to single with only an IPv6 address bound to it, vGW Series displays the following message

"The interface for management communications must have an IPv4 configuration, because Security VM SVM1 has only IPv4 interface."

- When your environment has a standby vGW Security Design VM that has only an IPv6 address bound to it, if you attempt to change the vGW Security Design VM from dual stack to single with only an IPv4 address bound to it, vGW Series displays the following message:

"The interface for management communications must have an IPv6 configuration, because there is a Standby Appliance with IPv6 interface."

**Related
Documentation**

- *Understanding vGW Series IPv4 and IPv6 Dual Stack Support*
- *Understanding IPv6 Addressing*
- *Understanding vGW Series IPv6 Support*
- *Understanding the vGW Security Design VM*

Configuring vGW Series Proxy Settings

You use the Settings module Appliance Settings > Proxy Settings page to enter information about a proxy server, if one is required to make outbound http/https connections. The Security Design vGW connects to the Juniper Networks update server to check for download software updates. If this VM does not have direct access to the Internet, a proxy can be used. All update communications uses HTTPS.

You enter the IP address, port, and user credentials for the proxy server on the Proxy Settings page. vGW Series sends HTTPS (TCP 443) requests to Juniper Networks vGW Internet update servers to pull the latest available software. vGW Series supports both IPv4 and IPv6 addresses for proxy servers.

**Related
Documentation**

- *Understanding vGW Series*

CHAPTER 18

Time

- [Configuring vGW Series Time Settings on page 143](#)

Configuring vGW Series Time Settings

You use the Settings module Appliance Settings > Time Settings page to specify the time zone and current time settings crucial to the proper operation of vGW Series and to specify settings for NTP servers.

It is essential that the vGW Security Design VM have the correct time zone and that it has access to an NTP server. All system logs, security logs, security policy deployment, and other data are time-stamped. If the time setting is not correct, these data will be marked with the wrong time. vGW Security VMs installed on ESX/ESXi hosts synchronize their time settings with that configured on the vGW Security Design vGW.

If you do not have an internal NTP server, you can use the preconfigured NTP servers or another Internet-based NTP server. vGW Series supports both IPv4 and IPv6 addressing for NTP servers.

Related Documentation

- [Understanding vGW Series](#)
- [Configuring vGW Series Proxy Settings on page 142](#)
- [Installing an Additional vGW Security Design VM and Configuring the Primary vGW Security Design VM to Use It for High Availability](#)

Backup and Restore

- [Understanding the vGW Series Backup and Restore Feature on page 145](#)
- [Configuring the vGW Series Backup and Restore Feature on page 147](#)

Understanding the vGW Series Backup and Restore Feature

Network and security groups at many companies typically backup and restore configurations for their hardware device systems. In fact for many organizations configuration backup is part of required configuration management practices.

To address this requirement for virtualized devices, vGW Series includes a feature that allows you to back up your vGW Security Design VM configuration to a file store or locally. When necessary, you can easily restore one of your backup versions.

You can run a modified version of the installation wizard that allows you to skip configuration settings that are backed up. After you run the installation wizard and log into the vGW Security Design VM, you can specify the vGW Security Design VM backup configuration to use from your backup location easily.

For details on how to configure settings for the backup and restore feature, see [“Configuring the vGW Series Backup and Restore Feature” on page 147](#).

If the vGW Security Design Center VM configuration that was backed up used a static IP address, the restored version of it has the same IP address. In this case, agents can begin to communicate with the restored vGW Security Design VM immediately after it is started. vGW Series supports both IPv4 and IPv6 addresses.

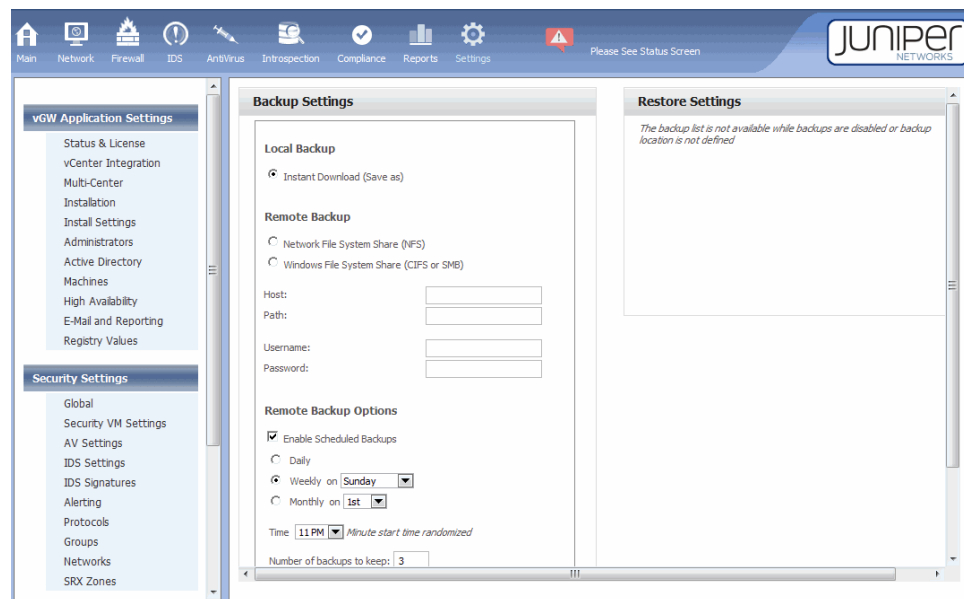
The issue is you can't use the 'Windows File System Share (CIFS or SMB)' option if you are using only IPv6. This option requires IPv4



NOTE: You cannot use the Windows File System Share (CIFS or SMB) option if you are using only IPv6. This option requires IPv4.

See [Figure 38 on page 146](#).

Figure 38: Settings Module Backup and Restore Settings



vGW Series backs up and restores the following content:

- All configuration information that you configured using the vGW Security Design VM, including:
 - machines
 - networks
 - groups
 - protocols
 - security policies objects
 - policies associated with groups
 - Smart Groups group membership and logic
 - Static Groups VM membership. Note that the VM-ID/UUID will change during the backup and restore process.
 - Administrator accounts. Administrator passwords are exported in a safe and secure manner.



NOTE: All source tables are backed up except those for connections, alerts, and idp_alerts. You must use another tool or process that copies the entire VM (vmdk) to back up that information.

The vGW Security Design VM backup-and-restore feature allows you to:

- Specify where to back up the files, locally or to a remote store.
- Specify the number of backup files to retain. You can remove all backup copies whenever you choose to.
- From among the backed-up versions, select the configuration to restore.
- Schedule when to back up the configuration.

Related Documentation

- [Configuring the vGW Series Backup and Restore Feature on page 147](#)
- [Understanding vGW Series](#)
- [Understanding the vGW Security Design VM](#)
- [Understanding the vGW Series Settings Module on page 3](#)

Configuring the vGW Series Backup and Restore Feature

vGW Series provides a backup and restore feature that you can use to create and store multiple backups of your vGW Security Design VM configuration and easily restore a backed up version. This topic explains how to configure settings for it. It also explains what you must do after you restore the vGW Security Design VM from a backup version. [Figure 39 on page 147](#) shows the Settings module Appliance Settings > System Settings Backup page that you use for this purpose.

Figure 39: Settings Module Backup and Restore Settings

The screenshot shows the Juniper Networks Settings Module interface. The top navigation bar includes icons for Main, Network, Firewall, IDS, AntiVirus, Intrusion, Compliance, Reports, and Settings. The left sidebar lists various settings categories under 'vGW Application Settings' and 'Security Settings'. The main content area is titled 'Backup Settings' and contains two sub-sections: 'Local Backup' and 'Remote Backup'. Under 'Local Backup', the 'Instant Download (Save as)' option is selected. Under 'Remote Backup', the 'Network File System Share (NFS)' option is selected. The 'Remote Backup Options' section includes a checked box for 'Enable Scheduled Backups', a frequency dropdown set to 'Weekly on Sunday', a time dropdown set to '11 PM', and a 'Number of backups to keep' field set to '3'. The 'Restore Settings' section on the right is currently empty, showing a message: 'The backup list is not available while backups are disabled or backup location is not defined'.

You can configure your system to back up the vGW Security Design VM in either of the following ways:

- **Local Backup:** This option backs up the vGW Security configuration immediately as an instant download, similar to a Save As function.

- **Remote Backup:** This option allows you to back up the vGW Security Design VM remotely at a scheduled time. You can also use it to back up the vGW Security Design VM now.



NOTE: You cannot back up the vGW Security Design VM over IPv6 networks.

To back up the vGW Security Design VM remotely:

1. In the **Backup Settings** pane under **Remote Backup**, specify where you want the backup to be stored. Select:
 - Network File System Share (NFS)
 - Windows File System Share (CIFS or SMB)

If you want to use the Windows Files System (CIFS (Common Internet File System) or SMB (Server Message Block) as the file store, specify the following information:

 - The name of the host and its path.
 - The username and password used to access the file share.
2. Configure the **Remote Backup Options**.
 - a. To schedule the backup, select **Enable Scheduled Backups**.
 - Specify the date and time:
 - For **Daily**, select it.
 - For **Weekly**, select the day.
 - For **Monthly**, select the date of the month.
 - In any of these cases, in the **Time** box, select the time when the backup should begin.
 - b. In the **Number of backups to keep**:, specify the number of backup versions to create and write to the file share.
3. Select **Backup before software update** to direct the vGW Series to back up the vGW Security Design VM before it is updated, whether the update is automatic or manual.
4. Click **Save** to save your backup configuration definition.
5. To back up your configuration immediately, click **Backup Now**.

The Restore Settings pane allows you to restore a backup file from the location where you stored the files.



NOTE: Clicking Restore causes the system to be restarted.

- To upload a local restore file, in the Local Restore section of the Restore Settings pane:
 1. Click **Browse...** to locate the backup file.

To clear the file selection, press **Clear**. Pressing Clear does not delete the backup file. It simply clears the browse box to allow you to select a different file.

2. Click **Restore**.

- To restore a backup file from a remote location, in the Remote Restore section of the Restore Settings pane:

1. Select a backup file from the list. The list identifies the name of the file, the date it was created, and the file size.

To refresh the Remote Restore configuration backup list, click **Retrieve File List**.

2. Click **Restore**.



WARNING: After you restore the vGW Security Design VM, you must reconfigure high availability (HA) for it. See the following procedure.

After you restore the vGW Security Design VM:

1. Verify that it is working properly.
2. Cancel the standby (secondary HA) vGW Security Design VM.
3. Reconfigure HA for the restored vGW Security Design VM.

For details on how to reconfigure HA, see *Installing an Additional vGW Security Design VM and Configuring the Primary vGW Security Design VM to Use It for High Availability*.

Related Documentation

- [Understanding the vGW Series Backup and Restore Feature on page 145](#)
- [Understanding vGW Series](#)
- [Understanding the vGW Security Design VM](#)
- [Understanding the vGW Series Settings Module on page 3](#)

CHAPTER 20

Logs

- [Understanding vGW Series Log Collection on page 151](#)
- [Viewing the vGW Series Logs on page 154](#)

Understanding vGW Series Log Collection

vGW Series Collection Tool allows you to generate log collections for the vGW Security Design VM and vGW Security VMs. You can generate log collections for:

- Only the vGW Security Design VM.
- One vGW Security VM.
- The vGW Security Design VM and one or more vGW Security VMs collectively from the same point of access.

In this case, you select the vGW Security VMs along with the vGW Security Design VM, and log collections will be generated for them also.

You can also generate log collections for a secondary vGW Security VM if you configured one for a vGW Security VM for high availability.

You can provide the log collection files to the Juniper Networks Support team to be used for diagnostic troubleshooting purposes. The Collection Tool is available on the Settings module Appliance Settings > Log Collection page.

- [Log Collection on page 151](#)
- [Generating the Log Collections on page 152](#)
- [Uploading the File on page 153](#)
- [Downloading the File on page 153](#)
- [Using a Method Other Than the vGW Security Design VM to Generate Log Collections for It on page 153](#)

Log Collection

For some reason you might encounter problems that necessitate troubleshooting the vGW Security Design VM itself and maybe one or more vGW Security VMs that exhibit problems. The Collection Tool allows you to generate information useful in solving the problem.

When you generate log collections for the vGW Security Design VM and vGW Security VMs together, they are included in a single compressed archive file. The (TGZ) zip file contains a separate zip for each component—a zip file for the vGW Security Design VM log collection and separate zip files for the log collections of each vGW Security VM that you selected. If no vGW Security VMs were selected, the zip file contains only the logs collected for the vGW Security Design VM.



NOTE: Because vGW Security VM log collections are copied to the vGW Security Design VM, it is recommended that you not initiate log collections for more than three vGW Security VMs concurrently. Although the recommendation is not a restriction, typically problems encountered are constrained to a small number of vGW Security VMs, so it should not be necessary to include a large number vGW Security VMs.

To remind you of the recommendation, vGW Series displays a confirmation alert after you have selected more than three vGW Security Design VMs.

After the log collections have completed, you can directly upload the file to a support server or you can download a copy of the file to submit to the Juniper support team manually. Juniper Networks recommends that you upload the file to the support server.

Generating the Log Collections

If you do not select the check box for any of the vGW Security VMs, vGW Series generates log collections only for the vGW Security Design VM. To take this action:

1. Click **Start New Collection**.

The resulting zip file contains only the vGW Security Design VM logs.

2. Follow the instructions in [Uploading the File or Downloading the File](#) to send the log collections to the Juniper Support team.

To use the Collection Tool to generate log collections for the vGW Security Design and one or more vGW Security VMs:

1. Select the **Get Logs** check box to the right of the name of each vGW Security VM for which you want to generate a log collection. The Collection Tool generates relevant log and system files and it compresses them in a TGZ zip file. The log collections are packaged together in a single zip file with the logs for the vGW Security Design VM.
2. Click **Start New Collection**.

The log collection process begins. The Collection Tool generates the log collection for all entities in parallel. When all the log collections are copied to the vGW Security Design VM, it shows a message of **Done! The log is now ready**.

You can either upload the file to the support center or download a copy of the zip file containing all the log collections to your local system to submit to the Juniper Support team manually.



NOTE: Juniper Networks recommends that you upload the file to the support server.

Uploading the File

When you click Upload in the Upload Log Collection pane, the newest zip file is uploaded, and an ID is returned to you. The upload process encrypts the file (through AES-256), and it transfers it to a protected server. Before you upload the file, briefly describe the problem in the comment field.

To upload the file:

1. Provide a brief description of the problem in the scroll box in the **Upload Log Collection** pane, and any other comments that you would like to submit.
2. Click **Upload**.

A **Submitting collection to support server....** progress message is reported. When the process completes, the message **Submission successful. Upload ID *id-number*** is displayed.

Make note of the ID, which you use to track your submission. You should refer to this ID in trouble tickets or other communication with the Juniper Networks support team about the problem.

Downloading the File

If you click **Download** in the **Download Log Collection** pane to download the file, you can send the file to Juniper Networks Support through e-mail at any time, or you can post the log collection to a server.

The downloaded file is called `datacollection-date.tar.gz`.

Using a Method Other Than the vGW Security Design VM to Generate Log Collections for It

When it is not possible to generate a log collection from the vGW Security Design VM, you can run the Collection Tool using another method. You can use this method to generate a log collection only for the vGW Security Design VM.

From the vGW command line interface (vGW CLI), you can use the `logs collect` command to generate log collections for the vGW Security Design. The command prints out the location of the file. You can then copy the file to another location using `scp`.

Related Documentation

- [Understanding vGW Series](#)
- [Understanding the vGW Security Design VM](#)
- [Viewing the vGW Series Logs on page 154](#)
- [Adding and Editing vGW Series Machines Definitions \(VMware\) on page 85](#)

Viewing the vGW Series Logs

You can use the Settings module Appliance Settings > Log Viewer to view system and application logs for basic system activity monitoring and troubleshooting. You can also select the number of lines that are displayed in the viewer.

**Related
Documentation**

- [Understanding vGW Series](#)
- [Understanding vGW Series Log Collection on page 151](#)
- [Adding and Editing vGW Series Machines Definitions \(VMware\) on page 85](#)

CHAPTER 21

Support

- [Understanding vGW Series Support Settings on page 155](#)

Understanding vGW Series Support Settings

You use the support section of the Settings module in the vGW Security Design VM to:

- reboot the vGW Security Design VM.
- restart vGW Series services.
- enable or disable debugging flags used for troubleshooting.

If you enable debug flags, return to this page after the log files are collected, and click **Debugging OFF**. When the debug setting is enabled, many log files are generated which could cause disk space usage problems.

Click Advanced in the Debug Flags pane to display a list of debug flags that you can set. For example, you can enable the active.directory flag to generate additional troubleshooting information in /usr/lib/tomcat/webapps/ROOT/log/debug.log.0.

- enable or disable SSH remote access to the vGW Security Design VM.

When you enable SSH, you can administer the vGW Series through an SSH client, such as PUTTY. This allows security teams to access the vGW command line of the vGW Security Design VM and the vGW Security VM components without having to use the vSphere Client.

When you access the vGW Security Design VM or vGW Security VM(s) through SSH, you are presented with a command-line interface. The command-line interface supports a variety of system options. Enter ? or enter **help** at the command-line prompt to view a list of supported vGW Series commands.

Related Documentation

- [Understanding vGW Series](#)
- [Understanding vGW Series Log Collection on page 151](#)

PART 5

Reports

- [Basics on page 159](#)
- [Reports Configuration on page 165](#)

CHAPTER 22

Basics

- [Understanding the vGW Series Reports Module on page 159](#)
- [Configuring a vGW Series Report on page 160](#)
- [Configuring Specifications for Automated Reports Using the vGW Series Reports Module on page 163](#)

Understanding the vGW Series Reports Module

The vGW Security Design VM Reports module allows you to create automated reports and modify parameters for creating them, and then view the results when a report is generated.

The Reports module includes the following tabs:

- Add/Edit Reports

You use this tab to create reports. By default, the Add/Edit Reports Tab page table is empty. After you create one or more reports, they appear in the table.

- Recent Reports

The Recent Reports tab displays a table containing previously created reports. To open a report, double-click the desired report in the list. You can open it as a PDF file, or you can save it to the hard drive.



NOTE: To display a report as a PDF file, there must be a PDF viewer installed on your system.

Reports are formatted with a high-level header that includes the report name and the date the report was created.

You can create the following types of reports by selecting them in the Report Selection section when you configure a report specification:

- Executive Summary

The Executive Summary report provides a broad view of security and performance reports across all vGW Security Design VM modules.

- Firewall

The Firewall report identifies the top accepted and rejected connections processed by vGW Series firewalls.

- Network Activity

The Network Activity report provides a summary of network usage, including the most active VMs and top protocols observed on the virtualized network.

- Security

Security Report

The Security report includes:

- Top destinations for connections denied by the firewall.
- Top sources of connections denied by the firewall.
- Most common IDS alerts seen in the virtual network.
- Top sources that generated IDS alerts in the virtual network.
- Top destinations targeted by IDS alerts.

- Introspection

The Introspection report provides details on the applications installed on the selected VMs, and it provides a breakdown of operating systems used. It also provides an Image Enforcer report that is generated when VMs are compared to a Gold Image, which is a valid and desirable template or VM.

- Compliance

The Compliance report provides a detailed status view of all compliance label groupings.

In addition to these report types, you can also create custom reports.

Reports and charts displayed in reports show both IPv4 and IPv6 addresses.

**Related
Documentation**

- *Understanding vGW Series*

Configuring a vGW Series Report

You can configure the vGW Security Design VM to produce reports on various aspects of your virtualized environment that is secured by vGW Series. You can create executive summary, firewall, network activity, security, Introspection and Compliance reports.

Reports and charts displayed in reports show both IPv4 and IPv6 addresses. In addition to current values, you can filter on IPv6 in reports.

When you add a new report, you must specify general information and the report destination and schedule information, as described in this procedure. For details on information that you configure for individual reports, see the topic for that report type.

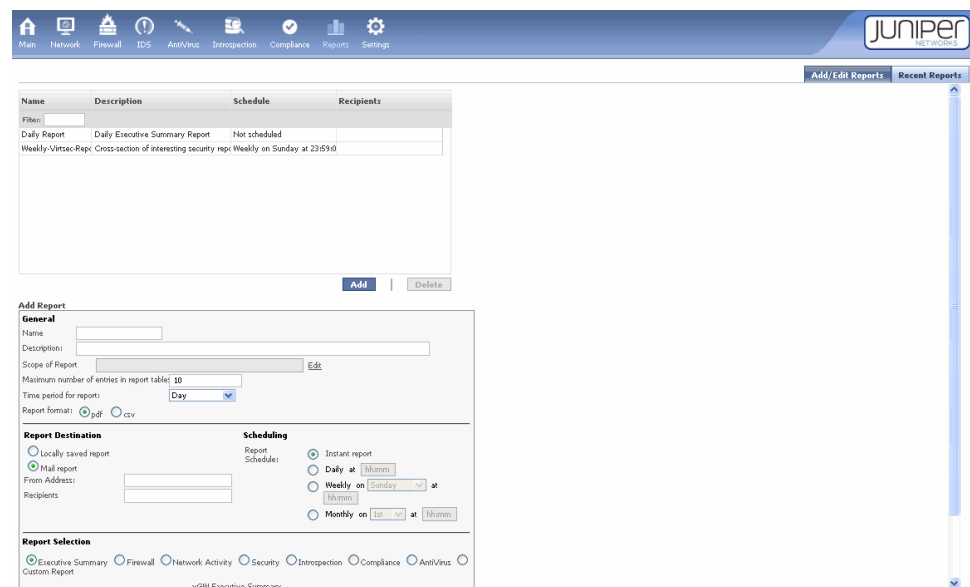
From the vGW Security Design VM Reports module:

1. Click **Add** beneath the list of existing reports. Enter the following information in the displayed Add Report pane. See [Figure 40 on page 161](#) and

Figure 40: Adding a vGW Series Report Using the Reports Module



Figure 41: Defining General, Destination, and Scheduling Information for the Report



2. In the General section, specify the following information:
 - a. In the Name field, give the report a name to identify it. This is the name that is displayed in the Name column of the reports table.
 - b. Add a description that identifies the report content. This description is displayed in the Description column of the reports table.

- c. In the Scope of report field, specify the VM groups that you want the report to cover. Click **Edit** to display a list of configured VM groups.
 - d. In the Maximum number of entries in report field, specify the record number limit.
 - e. In the Time period for report field, specify the period across which data is collected. Select **Day**, **Week**, or **Month**.
 - f. In the Report format field, select the option button for either pdf or csv to specify how you want the data formatted: as a PDF file or a CSV file.
3. In the Report Destination section, specify the following information:
- a. Whether to save the report file locally or send it to one or more recipients using e-mail.
- If you select the Mail report option button, specify the source address and the addresses of recipients that you want the report mailed to.

Figure 42: Configuring the Report Destination and Generation Schedule

The screenshot shows a configuration interface divided into two main sections: **Report Destination** and **Scheduling**.

Report Destination:

- There are two radio buttons: **Locally saved report** (selected) and **Mail report**.
- Below the radio buttons are two text input fields: **From Address:** and **Recipients**.

Scheduling:

- The label **Report Schedule:** is followed by three radio buttons: **Instant report**, **Daily at**, and **Weekly on** (selected).
- Below the **Daily at** radio button is a time input field labeled **hh:mm**.
- Below the **Weekly on** radio button, there is a day selector (currently showing **Sunday** with a dropdown arrow) and a time input field labeled **03:30**.
- Below the **Monthly on** radio button, there is a day selector (currently showing **1st** with a dropdown arrow) and a time input field labeled **hh:mm**.

4. Configure the report schedule.
 - To generate the report now, select the Instant report option button.
 - To generate a daily report, select the Daily at option button. In hours and minutes, specify the time when you want the report to be generated.
 - To generate a weekly report, select the Weekly on option button. Specify the day, week, and hour and minutes when you want the report to be generated.
 - To generate a monthly report, select the Monthly on option button. Specify the day of the month, and the time in hours and minutes.
5. In the Report Selection section, select the type of report to generate. You can configure the system to generate one or more types of reports. See [Figure 43 on page 163](#).

Figure 43: Configuring the Types of Reports to Generate

Administrators			Filter <input type="text"/>
Username	Full Name	Type	Authentication Type
admin	Default Global Admin	Global Admin, Console administrator	Internal
admin-security-examp	admin-security-example	VM Admin	Internal

Related Documentation • [Understanding vGW Series](#)

Configuring Specifications for Automated Reports Using the vGW Series Reports Module

This topic explains how to configure parameters that determine the kind of information to be generated in reports and when the reports should be generated.

To make report data more useful, you can use the Report Selection section to specify filters for the content. You can filter reports by Source IP, Destination IP, or Protocol. You can also filter out high, medium, and low priority alerts. Filtering allows you to report on exactly the information you need.

When you add a report specification, you can select predefined reports, including Executive Summary, Firewall, Network Activity, Security, Introspection, Compliance, and Smart Groups. You can also create custom reports.

To define a report:

1. Click **Add**.
2. Select the machines you want to report on, or select **All Machines** to report on the entire virtualized infrastructure.
3. Enter a name for the report and a description.



NOTE: Do not use spaces or special characters in the report name.

4. Specify the maximum number of entries for the report.
5. Specify the time period to report on.
6. Choose either PDF or CSV as the output format for the report.



NOTE: To display a report as a PDF file, a PDF viewer must be installed on the system.

7. Specify whether the report should be saved on the local hard disk or sent in e-mail to a recipient.



NOTE: If you use e-mail, you can specify to whom the report is sent, including an individual e-mail account, an e-mail alias, or multiple accounts separated by colons. You can also specify the e-mail address that will appear in the 'From' field on the e-mail.

8. Choose when to generate the report. You can direct the system to generate a report immediately, or you can schedule the report to run at a particular time and day.

We recommend that you schedule reports to run during low utilization periods, such as off hours. Report generation can consume significant system resources.

9. Choose a report type. Several predefined reports are provided, including Executive Summary, Firewall, Network Activity, Security, Introspection, and Compliance. You can also create custom reports.

A report selected during the report creation process has the title, graph, and relevant table data. If you select more than one type of report, each one is included in the same PDF output file, one after the other.



TIP: Select report type to display a description of the report.

10. Click **Generate Now** or **Save** to create the report.

Related Documentation

- *Understanding vGW Series*

CHAPTER 23

Reports Configuration

- [Understanding vGW Series Custom Report Types on page 165](#)
- [Understanding vGW Series Network Reports on page 166](#)
- [About the vGW Series Firewall Reports on page 166](#)
- [About the vGW Series IDS Reports on page 166](#)
- [About the vGW Series Introspection Reports on page 167](#)
- [Understanding the vGW Series Compliance Report on page 167](#)
- [Understanding the vGW AntiVirus Report on page 168](#)

Understanding vGW Series Custom Report Types

This topic identifies the kinds of custom reports that you can create using the Reports module of the vGW Security Design VM. When you create a custom report, you can choose specific parameters for Network, Firewall, IDS, Introspection, and Compliance reports. Alternatively, you can use the Report Selection section of the Add Report page to select predefined reports. The core attributes of these report types are provided in the predefined reports. For an overview of the Reports module, see [“Understanding the vGW Series Reports Module” on page 159](#).

The following topics describe the kinds of custom reports that you can define:

- [Understanding vGW Series Network Reports on page 166](#)
- [About the vGW Series Firewall Reports on page 166](#)
- [About the vGW Series IDS Reports on page 166](#)
- [About the vGW Series Introspection Reports on page 167](#)
- [Understanding the vGW Series Compliance Report on page 167](#)

Related Documentation

- [Understanding vGW Series](#)

Understanding vGW Series Network Reports

This topic describes the kinds of network reports you can define using the Reports module of the vGW Security Design VM. Before you read this topic, read [“Understanding the vGW Series Reports Module” on page 159](#).

- Top Talkers: Shows the machines generating the most traffic (combined source and destination traffic flows).
- Top Destinations: Shows where the systems are most frequently communicating.
- Top Protocols: Shows the most popular protocols in use on the virtual network.
- Top Sources: Shows which systems are generating the most traffic.
- Total Bytes: Similar to the Top Talkers report, but also shows which protocols are being used.

Related Documentation

- [Understanding vGW Series](#)

About the vGW Series Firewall Reports

vGW Series generates Firewall reports by pulling information collected by the Firewall module. You can define firewall security rules for the VMs. When connections are made to or from the resources, the firewall logs the activity and makes it available to the Reports module.

You can create the following firewall security reports:

- Top Accepted Destinations: Shows which machines in the destination field are accepting the highest number of connections, including source and destination fields for each firewall logging event.
- Top Accepted Sources: Shows the machines in the source field that are accepting the highest number of connections.
- Top Dropped or Rejected Destinations: Shows the machines in the destination field that are dropping or rejecting the highest number of connections. An action rule in a policy rule can be Accept, Drop, or Reject.
- Top Dropped or Rejected Sources: Shows the machines in the source field that are dropping or rejecting the highest number of connections.

Related Documentation

- [Understanding vGW Series](#)

About the vGW Series IDS Reports

vGW Series generates IDS reports by pulling information collected by its IDS module. These reports display a complete listing of all malicious or suspicious traffic on the virtual network.

- Top Alerts: Shows alerts seen on the virtual network
- Alert Sources: Shows sources of attacks.

The Maximum number of systems to include in the report determines how many attacks are reported. For example, if you specified a value of 20, and 20 attacks occurred on those systems but a total of 40 attacks occurred in the specified time period, only 20 attacks would be reported.

Related Documentation

- *Understanding vGW Series*

About the vGW Series Introspection Reports

vGW Series generates Introspection reports by pulling information that was collected by the Introspection module. These reports contain the following information:

- Known Applications: Applications that you define in the Introspection module as Known. Usually they are considered good and allowed in the virtualized environment.
- Unknown Applications: Applications that you have determined need further investigation.
- Bad Applications: Applications that you have defined as bad and that are not allowed in the environment.
- Unclassified Applications: Applications that you have not classified. By default, a state of Unclassified indicates that the vGW Series discovered an application on a VM that it does not recognize.
- Operating Systems: Shows operating systems installed on VMs in the environment. vGW Series collects operating system information automatically, enabling you to run a report on all operating systems in the environment.

Related Documentation

- *Understanding vGW Series*

Understanding the vGW Series Compliance Report

vGW Series generates Compliance reports by pulling information collected by the Compliance module. These reports display information from the following compliance groupings:

- DISA: Shows information related to Defense Information Systems Agency best practices.
- NSA: Shows information related to National Security Agency best practices.
- PCI: Shows information related to Payment Card Industry best practices.
- VMware: Shows information related to VMware security best practices.

The resulting report shows three different summary tables containing information related to one or all of the these compliance groupings. For example, if you select just PCI and VMware, the report will contain three tables that show the values for those two

compliance groupings. The first table shows all rules occurring in the selected groupings. The second table shows the groupings with summary information on rules, number of VMs, and status. The third table shows all VMs associated with the groupings.

Related Documentation

- *Understanding vGW Series*

Understanding the vGW AntiVirus Report

You can use the Reports module of the vGW Security Design VM to define and schedule vGW AntiVirus reports.

You can specify that the following information be included in the report:

- AntiVirus Alerts
- AntiVirus Quarantine
- AntiVirus Summary

You can specify that the report data is to be sorted by threat type, threat name, or VM.

For details on standard report configuration information that applies to AntiVirus, see [“Understanding the vGW Series Reports Module” on page 159](#).

Related Documentation

- *Understanding vGW Series*

PART 6

Index

- [Index on page 171](#)

Index

Symbols

#, comments in configuration statements.....	xiii
(), in syntax descriptions.....	xiii
< >, in syntax descriptions.....	xii
[], in configuration statements.....	xiii
{ }, in configuration statements.....	xiii
(pipe), in syntax descriptions.....	xiii

A

administrators	
changing passwords.....	79
defining and adding.....	79
appliance status.....	9
Application Settings.....	7
authentication	
changing passwords for administrators.....	79
Auto Deploy.....	25
VMware.....	26

B

backup and restore.....	145, 147
braces, in configuration statements.....	xiii
brackets	
angle, in syntax descriptions.....	xii
square, in configuration statements.....	xiii

C

comments, in configuration statements.....	xiii
conventions	
text and syntax.....	xii
curly braces, in configuration statements.....	xiii
customer support.....	xiii
contacting JTAC.....	xiii

D

database status.....	9
delegate centers.....	63
documentation	
comments on.....	xiii

F

font conventions.....	xii
-----------------------	-----

G

Groups.....	111
-------------	-----

I

IPv4	
defining network objects.....	131
IPv6	
defining network objects.....	131

L

licenses	
evaluation.....	10
features.....	10
managing.....	11
requirements.....	10
understanding.....	9
wizard.....	11
log collection.....	151

M

machines.....	85
manuals	
comments on.....	xiii
multi-center feature.....	63

N

network objects.....	131
Networks page.....	131

P

parentheses, in syntax descriptions.....	xiii
policy	
for multiple vNICs on the same VM.....	47
Policy per vNIC	
settings.....	47
Primary-level entry	
secondary-level entry.....	66
Primary-level entry only.....	66

R

reports.....	160
Reports module	
AntiVirus.....	168

S

Security Settings	
Groups.....	111

Settings module	
Application Settings.....	7
machines.....	85
overview.....	3
settings module	
multi-center.....	63
Smart Groups.....	114
Groups.....	111
status	
appliance status.....	9
database status.....	9
support, technical See technical support	
syntax conventions.....	xii
 T	
technical support	
contacting JTAC.....	xiii
 U	
Updating system components.....	135
vGW Security Design VM.....	135
vGW Security VM.....	135
 V	
vCenter	
settings.....	37
vGW Security Design VM	
vGW Security VM Settings.....	97
vGW Security VM Settings.....	97
vGW Series.....	25, 26
VMware Auto Deploy support.....	25, 26
VMware	
integrating vGW Series.....	37